Boolean Functions and their Applications
Loen, Norway, June 17-22, 2018.

Report for COINS Research School
by Diana Davidova

The theird international conference on Boolean Functions and their applications took place at Loen, Norway from 17th to 22 June 2018.The aim of workshop is 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 further explore their applications in cryptography, error correcting codes and communications.

All of the topics of the conference was related to my current research in University of Bergen. I want to mention some of them.

The conference starts with talk of my collegue from Unverity of Bergen, Marco Cardelini. The topic of him talk is "On relations between CCZ and $EA-$equivalences". First he discussed relations between $EA-$-equivalence and $CCZ-$equivalence, and some of their properties. He presents a procedure which allows to investigate if the $CCZ-$equivalence leads to more functions than applying $EA-$equivalence and the inverse transformation (when it is possible), for the case of non quadratic functions. At the end he gave the classification of APN functions. There are twelve classes of APN functions which are $CCZ-$inequivalent to power functions.Hel show that only 10 of this 12 classes are distinct. Precisely, two of these 12 families (defined for n even) are a particular case of the hexanomials introduced by L. Budaghyan and C. Carlet.

An interesting talk of the first day was given by Christina Boura from UVSQ Versailles, France. The topic is "On Sboxes sharing the same DDT". This work is a join work with Anne Canteaut, Jeremy Jean and Valentin Suder. This work focuses on two different equivalence notions for vectorial Boolean functions, which are calledl DDT and $\gamma-$equivalence. They proved that the number of elements in the differential equivalence class of a function is invariant under CCZ-equivalence. During the talk was provided an algorithm for computing the differential equivalence class corresponding to a prescribed DDT. Using this algorithm they found permutations F whose differential equivalence classes contain other elements than the functions $x \mapsto F(x \oplus c) \oplus d$. She made a conjecture that this is only the case when some rows of the corresponding DDT are equal.

Also I want mention talk of Natalia Tokoreva from Sobolev Institute of Mathematics, Novosibirsk. The title of her talk is " Algebraic normal form of a bent function:what is it? " Bent functions can be defineined in two ways: in terms of maximum distance to all affine functions and in the terms of Walsh Hadamard transform. But we don't have properties of algebraic normal form (ANF) of bent functions. Natalia presents a collection of properties of ANF, which allows us to conclude that given function is bent.

One of theorganizers of the conference , Claude Carlet from the Univesity of Paris 8, had a talk on the topic " Low-weight correlation-immune Boolean functions for counter-measures to side channel attacks". the known constructions of resilient functions are based on the Walsh transform, he proposed construction of low-weight CI functions based on the Fourier-Hadamard transform. The resulting constructions are very different, howeverthese two transforms are closely related.

I am appreciated a lot to COINS for the opportunity to participate in such interesting and useful event.