Boolean Functions and their Applications

16-21 June, 2019, Florence, Italy

Report for COINS Research School
by Diana Davidova

The international conference Boolean functions and their applications, organized by the Selmer centre of the Universiy of Bergen, took place in Florence, Italy from 16 to 21 of June, 2019. Starting from 2017 Boolean functions and their Applications (BFA) workshop is an annual event. In 2019 it was 4th conference. This year the conference was dedicated to 70th anniversary of Claude Carlet. The topics of the conference include all the discrete structures used in error correcting coding, cryptography or communications. There was 12 planar talks and 27 ordinary talks.

Among the planar speakers, was Claude Carlet itself. He is a formal member of Selmer Center, UIB and works in the University of Paris 8. The title of him talk was "Recent uses and problems on Boolean and vectorial functions". Among the people working in areas related to Boolean functions it is well-known that Claude Carlet was working that time on the final version of

him book dedicated to Boolean and vectorial boolean functions. In his talk he represents some of the chapters of the book devoted to the topic which pops up recently. More precise, Physical attacks and related problems on functions and codes;Fully homomorphic encryption and related questions on Boolean functions; Local pseudorandom generators (the Goldreich pseudorandom generator) and related criteria on Boolean functions; The Gowers norm on pseudo-Boolean functions.

The first two talks of the conference were planar talks by a members of the Selmer Centre and organizers of the BFA, Tor Helleseth and Lilya Budaghyan. Prof. Tor Helleseth's talk title is "Differential spectrum of non-binary Kasami power function and related topics". Kasami power functions are functions with low differential uniformity, which is very attractive for cryptography, sequence design and coding theory. Finding the complete differential spectra of permutation power functions is in general a much harder problem than just finding their differential uniformity. In the talk Prof. Helleseth determined complete differential spectra of Kasami power function in non-binary case. Prof. Lilya Budaghyan had a talk with title "On the Carlet-Charpin-Zinoviev Paper". In this paper of three authors was introduced a new equivalence relation on vectorial boolean function, the most general known up today. After the paper were published, this equivalence relation was called by the first letters of the paper's authors: CCZ-equivalence. The classification of boolean(vectorial) functions are made up to CCZ-equivalence. This work and, and in general, prof. Claude Carlet had a great impact on the career of Lilya, and not only to her.

I want to mention also the talk of Daniel Panario from Carleton University (School of Mathematics and Statistics) He was talking about ambiguity, deficiency and differential spectrum of low degree normalized permutation polynomials over finite fields. He represent the exact formulas for the ifferential spectrum, deficiency and ambiguity of all normalized permutation polynomials of degree up to six over finite fields.

A very interesting talk was given by Emmanuel Prouff. He was Ph.D. student of Claude Carlet, but decided to leave the research and go to the industry. Him talk was more related to practice and application and this makes it attractive. He was talking about a very hot topic, side channel analysis and the title of him speech was "Algorithmic Approaches to Defeat Side Channel Analysis". A countermeasure for side channel attacks consists in randomly splitting every sensitive intermediate variable occurring in the computation into several shares. The number of the shares, called masking order is a security parameter. Recently, there were introduced a several masking schemes, which can be used for arbitrary functions and orders. During the talk he discussed some issues and present some ideas to solve them.

Finally, I would like to mantion that I met a lot of interesting people, researchers on the conference. We discussed different problems related to our research field. The place of the conference was very beautiful, tasty food and interesting excursions by the surroundings of Florence. **I am appreciated a lot to COINS for the opportunity to participate in such interesting and useful fo my future career event.**