The 2nd International Workshop on **Boolean Functions and their Applications (BFA)**

Irene Villa

03-08 July 2017
Os, Norway

In July COINS supported me to attend *The 2nd International Workshop on Boolean Functions and their Applications (BFA)*. The workshop was held in Os, south of Bergen, from the 3rd to the 8th of July.

The aim of the workshop was to provide a forum for researchers whose work is on discrete functions and structures (Boolean functions), to give them an opportunity to exchange ideas, interests in open problems and to explore their application in cryptography, error correcting codes and communications.

Full program of the workshop, among with the abstract and the presentation slides of the talks given, can be downloaded from the event web-page (http://people.uib.no/chunlei.li/workshops/BFA2017/).

During the conference many interesting talks were given. Among them many were focused on the *Almost Perfect Nonlinear* property (APN) and on the *big APN problem*, finding an APN permutation in an even dimension greater than 6.

On the first day the fist talk given was by Kaisa Nyberg, from Aalto University, Finland, about linear approximations and their linear and statistical independence. In the rest of the morning we had an overview on APN permutations by Marco Calderini, a talk about S-box reverse-engineering: from cryptanalysis to the big APN problem by Léo Perrin and a talk on APN functions EA-equivalent to permutations by Valeriya Idrisova. Among

the talks given in the afternoon Claude Carlet, from University of Paris 8, presented a work on possible exponents of APN power functions and their relation with Sidon sets and sum-free sets. From ENS and PSL Research University (France), Pierrick Meaux's talk was about symmetric encryption scheme adapted to fully homomorphic encryption scheme: new criteria for Boolean functions. From Inria Paris Anna Canteaut talked about resistance of a block cipher against invariant attack.

On the second day Pante Stanica (Naval Postgraduate School, USA) talked about generalized Boolean functions. Patrick Solé, from Telecom ParisTech, presented a work on orthogonal group and Boolean functions. Moreover many presentations were focused on the *bent* property of Boolean function. Among them Bimal Mandal's work was on orthogonal group and Boolean functions, Wilfried Meidl talked about new classes of generalized bent functions and Natalia Tokareva, from the Russian Academy of Science, gave an overview of bent Boolean functions.

On the last day Alexander Pott (Otto-von-Guericke-University, Germany) talked about the duality of bent functions in odd characteristic. From ITMO University in Russia, Alla Levina's presentation was about wavelets transformation. Other talks were given and among them also two on *quantum* cryptography: Ashley Montanaro (University of Bristol) presented an overview on Boolean functions in quantum cryptography and Matthew G. Parker (UiB) talked about Boolean functions in a message-passing, quantum, and machine learning context.

Most of the topics treated during these days of conference were included in my research area (APN Boolean functions) or really close. Others, even if they were not strictly related to my current work, were still very interesting. In particular it was interesting to see different ways a Boolean function can be seen and studied, different approaches and different applications. Moreover I had the chance to meet some of the "big" names in this field!

Thanks to COINS that gave me this useful opportunity!