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

Irene Villa

17 - 22 June 2018
Loen, Norway

From the 17th to the 22nd of June the third international workshop on Boolean Functions and their Application was held in Loen. Like for its past editions, the aim of the workshop was to provide a forum for researchers who are working on discrete functions and structures, give them the opportunity to exchange ideas and open problems and explore the applications in cryptography, error correcting codes and communications.

The conference was thought to cover many topics, among those

- foundational theory of Boolean functions and discrete structures,
- the design, proposal, and analysis of cryptographically significant vectorial Boolean functions,
- the theory and construction of quantum Boolean functions,
- the theory of finite fields and its applications in cryptography and coding theory.

Many interesting talks were given during the days of the conference.
Professor Claude Carlet, from the University of Paris 8, gave a talk with the title *Low-weight correlation-immune Boolean functions for counter-measures to side channel attacks*. Correlation-immune functions are such that they keep the same output distribution when a number of input variables is fixed. Such maximal number is called the correlation immunity order of the function. Such good functions have been used in stream ciphers as combiners to allow the resistance to some specific attack. Recently correlation-immune functions are used in the context of side channel attacks.
Professor Massimiliano Sala, from the University of Trento (Italy) presented a work on *Computational aspects for the nonlinearity of Boolean functions*. In his presentation he gave a review of some known methods to compute the non-linearity of Boolean functions, beginning with the most classical

approach via the Walsh transform up to other approaches based on multivariate polynomial techniques, including Groebner basis computations.
Lauren De Meyer, from the University of Leuvem (Belgium) talked about *Classification of Balanced Quadratic Fucntions*. She presented a highly efficient algorithm that classify all n-bit permutations and also all balanced $n \times m$-bit functions for $m \leq n$. The algorithm allowed to generate all 5-bit quadratic vectorial Boolean functions in six minutes and enabled a complete classification of balanced 6-bit quadratic functions.
Luís Brandão, from the National Institute of Standards and Technology (NIST) in USA, gave a talk with title *On the Multiplicative Complexity of Symmetric Boolean Functions*. The multiplicative complexity of a Boolean function is the number of AND gates that are necessary and sufficient to implement the function over the basis {XOR, AND, NOT}. He presented some results on the multiplicative complexity for Boolean functions with twin variables. Showing that any nonlinear symmetric Boolean function is affine equivalent to a Boolean function with twin variables, he provided new upper bounds on the multiplicative complexity of symmetric Boolean functions up to 9 variables.

I am very grateful to COINS that gave me the support to attend this conference and gave me the chance to meet many interesting researchers from all over the world.