Boolean Functions and their Applications (BFA) 2018
Reflection report

Nikolay Kaleyski

December 4, 2018

1 Background

The third international workshop on Boolean functions and their applications (BFA) took place in at the Alexandra hotel in Loen between June 17 and June 22 2018. Located in the county of Sogn og Fjordane, Loen proved to be not only a convenient and comfortable place to host a conference, but also one of the most beautiful places in beautiful Norway, fusing together sublime mountain views with tranquil scenery in a natural harmony to delight both the eyes and the mind. Much the same can be said for the program of the workshop itself, which brought together a number of researchers studying various aspects of the theory and practice of Boolean functions, and allowed them to present their work, which resulted in one of the most varied and interesting conferences in the field that I have had the pleasure to attend to this moment.

Below, I will present a slightly more detailed description of two of the talks that I found particularly interesting and that are most relevant to my own research at the moment. This is, of course, not meant to be an exhaustive list, as virtually all the presentations at the BFA were quite excellent and touched on some aspect of Boolean functions or another. A full list of the talks, with abstracts and slides, can be found at `https://people.uib.no/chunlei.li/workshops/BFA2018/program.html`.

I also had the opportunity to present my research at the workshop by giving a talk entitled "Changing points in APN functions". Some of my colleagues from the department gave very informative presentations as well, which were especially relevant to me as we all work on similar problems. In addition, I was able to meet with some of my co-authors and to discuss current and future research.

Overall, this year's BFA was a very productive and pleasant experience in all aspects, and I am grateful to COINS for providing the financial support which allowed me to visit Loen and to take part in this amazing event.

2 Overview of Selected Talks

2.1 Leo Perrin

One of the most interesting presentations of the conference for me was held on the first day by Leo Perrin from Inria Paris, who gave a talk with the title "On CCZ-Equivalence, Extended-Affine Equivalence and Function Twisting". Since the number of Boolean functions grows extremely rapidly with the dimension of bits, different notions of equivalence, such as EA- and CCZ-equivalence, are defined which preserve some of the important cryptographic properties of the functions. Then only a single representative from each class has to be studied, thereby reducing the number of functions that have to be examined and facilitating their classification. CCZ-equivalence is more general than EA-equivalence, and functions are typically partitioned into CCZ-equivalence classes since this is easier to do. However, some properties of these functions, including some metrics which I am currently studying as part of my own research, are not preserved by CCZ-equivalence (only by EA-equivalence) and thus each CCZ-equivalence class has to be partitioned into EA-equivalence classes in order for a complete classification to be made. Leo Perrin's research concentrates exactly on this aspect, and answers the question: what needs to be added to EA-equivalence in order to allow us to describe CCZ-equivalence? The answer lies in a special operation called "function twisting", which allows one to move between the different EA-equivalence classes within a CCZ-equivalence class. An upper and lower bound on the number of these EA-equivalence classes are also derived from the author's theoretical framework, and the results are applied in practice in order to show e.g. that a 16-bit APN quadratic function cannot be CCZ-equivalent to a permutation.

In short, this was an excellent talk which shed some light on a known problem in the study of Boolean functions, and which was particularly interesting to me as it can be applied to my own research. I am currently in the process of reading the author's preprint on the same topic, and I believe that this work promises to be very useful to me.

2.2 Anastasiya Gorodilova

Another interesting talk was given by Anastasiya Gorodilova from Novosibirsk. The title of her talk was "Differential equivalence of APN functions: results and open problems", and focused on a new kind of equivalence between Boolean functions invented by the author, according to which two vectorial Boolean functions F and G are said to be equivalent if their associated Boolean functions γ_F and γ_G (with the value of e.g. $\gamma_F(a, b)$ indicating whether the equations $F(x) + F(a + x) = b$ has solutions or not). This is also of interest to me, as my research is currently focused on the differential properties of Boolean functions, and the behavior of γ_F for an APN function F is something that I have previously studied. The author also presented a number of open problems in her talk, which may be viable directions for future research.