Boolean Functions and Their Applications (BFA)
June 16 - June 21, 2019

Nikolay Kaleyski

The fourth international workshop on Boolean functions and Their Applications (BFA) took place between June 16 and June 21 2019 at the Villa Finaly just outside Florence, Italy. The workshop did not deviate from the established tradition, and provided a unique platform for researchers interested in Boolean functions to congregate and present their research.

The talks given by the participants were quite varied and very interesting, exploring different aspects and applications of Boolean functions and other related mathematical structures. A number of the presentation were dedicated to the cryptographic properties and applications of Boolean function; several researchers discussed relations between Boolean functions and coding theory, which is another crucial part of information security alongside cryptography; and a number of talks were dedicated to combinatorial designs, equations over finite fields, and other topics that either utilize Boolean functions, or, conversely, are used in the construction and analysis of Boolean functions.

In the following, I outline three talks that I found particularly interesting, and which illustrate the varied spectrum of topics discussed at BFA.

Jiří Pavlů (with Faruk Göloğlu) gave a talk entitled “Search for APN Permutations Among known APN Functions”. Their research is related to arguably the most important open problem in the study of cryptographic Boolean function, which is the existence of almost perfect nonlinear (APN) permutations on an even number of bits. APN functions provide the best possible resistance to differential cryptanalysis, which makes them very desirable to use in the design of block ciphers. However, the APN-ness of a function seems to be in conflict with another very natural and desirable property, namely that of being a permutation. To date, only one APN permutation (on 6 bits) is known. Whether APN permutations exist on 8 bits (which is easily the most significant case in practice), or on any even number of bits larger than 6, remains a mystery for the time being.

Several notions of equivalence are defined on the set of Boolean functions, one of which is the so-called Carlet-Charpin-Zinoviev equivalence, or CCZ-equivalence. The aforementioned APN permutation on 6 bits was found by traversing the CCZ-equivalence class of a previously known APN function which was not itself a permutation. This naturally suggests that further APN permutations could potentially be found by exploring the equivalence classes of other known APN functions. Unfortunately, this is extremely difficult to do, as the equivalence classes are huge and nigh intractable even for a relatively small number of bits. Existing necessary conditions for the equivalence of a function to a permutation are also extremely difficult computationally.

The authors consider one such necessary conditions, and derive a weaker but more computationally efficient necessary conditions for equivalence to a permutation. They utilize this necessary condition and run computational experiments on the known APN functions on up to 12 bits. Despite the conditions being weaker, this, perhaps surprisingly, is enough to prove that none of these functions is equivalent to a permutation (except for the isolated case on 6 bits mentioned above).

Pavol Zajac (with Matúš Jókay and Peter Špaček) talked about the “Linear and Differential Properties of S-boxes with Respect to Modular Addition”. Differential cryptanalysis, which was already mentioned above and which is one of the most powerful attacks against block ciphers, exploits dependencies between the difference of two inputs and the difference of their corresponding outputs. The notion of difference is expressed using the exclusive or (XOR) operation, on which the designs of most ciphers are based on.

The authors consider an alternative differential cryptanalysis in which the notion of difference is express using ordinary modular addition instead of XOR. A statistic measuring the resistance of a function to this kind of cryptanalysis is introduced as an analogue to the differential uniformity used to measure the resistance against classical differential cryptanalysis, and a number of computational experiments are performed in order to estimate how the known cryptographically secure functions behave with respect to this new statistic. Similarly, an analogue to nonlinearity (which measures the resistance to so-called linear cryptanalysis) is defined and studied in order to measure the resistance to a “modular” version of linear cryptanalysis.

Although the practical implication of this “alternative” kind of cryptanalysis (and hence the importance of the statistics introduced and studied by the authors) is still unclear, this was rather memorable talk as it introduces a novel element to a well-established approach that most are familiar with.

Last but not least, I would like to briefly mention the very interesting invited of Sihem Mesnager entitled “Equations over the Finite Field $\mathbb{F}_{2^n}$”. The contents does not deal with Boolean functions at all, but rather with the solutions of the equation $x^{2^k+1} + x + a = 0$ in the finite field $\mathbb{F}_{2^n}$ with $\gcd(k, n) = 1$. This is hardly surprising, as proofs of the cryptographic strength of Boolean functions can be quite technical in general, and more often than not amount to finding the set of solutions (or, at least, their number) of some equation over a finite field, such as the aforementioned one. Despite the deceptively simple form of such equations, finding (or counting) their solutions can, in general, be an extremely complicated task, spanning many years of research. For this reason, results such as the one presented here, are of immense interest to those working on Boolean functions, and on topics related to finite fields in general: not only does such a result constitute a noteworthy mathematical achievement in its own right, but it supplies researchers with a useful tool for handling equations that are likely to pop in the analysis of i.a. cryptographic functions.

The above summary does by no means exhaust the wide array of topics and ideas discussed at the workshop, but doing so would be practically impossible without writing a detailed report of each individual talk. To reflect the significance and excitement of the event, it hopefully suffices to mention that presentations were given by prominent authorities in the field, such as Claude Carlet, Robert Coulter, Daniel Katz, and Daniel Panario, among others, with a number of talks given by representatives of UiB such as Lilya Budaghyan, Marco Calderini, Tor Helleseth, and Chunlei Li. A full list of the talks can be found on the official pages of the coherence at https://boolean.w.uib.no/bfa-workshops/bfa2019/program/.

To conclude, the BFA 2019 workshop has been both very pleasant and very useful to me professionally, giving me the opportunity to meet some of my close collaborators in person, as well as to listen to a number of inspirational talks and accumulate new information for my own research. I am thus grateful to COINS for providing me with the opportunity to attend such a wonderful event.