Reflection report for

BFA 2019 : The 4th International Workshop on Boolean Functions and their Applications

Irene Villa

16 - 21 June 2019
Florence, Italy

During the third week of June, in the beautiful city of Florence in Italy, the 4th International Workshop on Boolean Functions and their Applications took place. This year workshop was dedicated to the 70th birthday of professor Claude Carlet, from the University of Paris 8. His work, still very prolific, has been of fundamental importance in many different areas related to Boolean functions and vectorial Boolean functions.

The workshop, now at its 4th edition, has the aim to create the opportunity for young researchers and more experienced professors to meet and discuss about Boolean functions and all the areas that are related to it. Indeed many applications are in the area of error correcting coding, cryptography and communication.

Every day of the workshop different talks given by well known invited speakers were given. Also many other talks were given by participants with an accepted abstract. The workshop was quite international. Indeed considering all the participants, around fifty people, there were people coming from US, Canada, Europe, Russia and China.

In the following a brief description of some of the talks given during the workshop.

- Professor Claude Carlet gave a talk on *Recent uses of Boolean and vectorial functions and related problems*. In particular he introduced some physical attacks and the related problems on functions and codes. He mentioned, talking about side channel attacks (SCA), some countermeasures that were implemented for block ciphers in order to be resistant to SCA.

- Emmanuel Prouff, from ANSSI the National Cybersecurity Agency of France, presented a work on *Algorithmic Approaches to Defeat Side Channel Analysis*. To defeat SCA a common countermeasure consists in randomly splitting every sensitive intermediate variable occurring in the computation into several shares. The number of such shares plays a role in the security of the algorithm. He presented and compare some of the state-of-the art methods and the techniques used to analyse their security.

- René Peralta, from NIST the National Institute of Standards and Technology, had a presentation with title *Research Directions on the Complexity of Boolean Circuits for Codes and Cryptography*. The circuit complexity of Boolean functions is of fundamental interest for practical cryptography: the number of non-linear gates in a Boolean circuit has direct impact on the efficiency of high-level cryptographic primitives and on the size of the corresponding side-channel resistant circuits, the number of linear gates directly impacts the cost of hardware implementations. There were presented some of recent results in obtaining new recurrence relations for binary polynomial multiplication, finding new constructive bounds for multiplicative complexity of symmetric Boolean functions and improving the complexity of Reed-Solomon codes.

- Nicolas Courtois, from UCL the University College London, talked about *On the Existence of Boolean Functions Resistant Against Non-Linear Invariant Attacks*. Recent papers show how to construct polynomial invariant attacks on block ciphers for certain Boolean functions. He showed the existence of Boolean functions which seem quite resistant to such attacks.

- Nian Li, from Hubei University in China, presented a work on *Constructions of linear codes from cryptographic functions*. Linear codes have a wide range of applications in several areas: data storage systems, communication systems, consumer electronics products, etc. Indeed their algebraic structure can be analysed and they are easy to implement in hardware. He introduced some methods to construct linear codes by using cryptographic functions and he presented some research problems in the area.

I am very grateful to COINS that gave me the opportunity to attend this event. Indeed, during the week of the workshop, I had the chance to talk about my current work with some of the participants whom gave me ideas and suggestions on how to continue the research.