International Conference in honor of Professor Claude Carlet Codes, Cryptology and Information Security

Irene Villa

10-12 April 2017
Rabat, Morocco

These three days of conference, made in honor of Professor Claude Carlet from the University of Paris 8, France, were focused on the theory and applications of cryptographic techniques, coding theory, and information security, fields in which the Professor gave a great contribution. Many talks were given during the conference and many of them were closely related to my research area. In the following I will briefly describe some of these talks.

Some Results on the Known Classes of Quadratic APN Funcions.
An overview of what is known so far about APN Vectorial Boolean functions and new results obtained in their classification and their equivalence relations.

Codes for Side-Channel Attacks and Protections.
A revisit of side-channel analysis from the standpoint of coding theory. The main results obtained through this analysis were presented and also some optimal strategy of attack in various practical context.

New Bent Functions from Permutations and Linear Translators.
New advances about the classification of bent functions, important elements in cryptography due to their high resistance to linear cryptanalysis. New infinite families of such permutations were presented.

Bent Functions in $\mathcal{C}$ and $\mathcal{D}$ Outside the Completed Maiorana-McFarland Class.
Conditions related to bent functions, their classification and their construction. There are given some existence results for bent functions that don't belong to the completed Maiorana-McFarland class.

Quantum Algorithms Related to HN-Transforms of Boolean Functions.
A generalization of an algorithm was proposed. It can be used to distinguish different classes of Boolean functions over and above what is possible by the original algorithm.

Explicit Characterizations for Plateaued-ness of p-ary (Vectorial) Functions.
Some more general results are given on plateaued functions defined over fields

of generic characteristic p.The family of plateaued functions contains bent functions.

Somewhat/Fully Homomorphic Encryption: Implementation Progresses and Challanges.
An overview of the efforts made to secure and implement Somewhat/Fully Homomorphic Encryption ((S/F)HE) schemes and the problems to be tackled in order to progress toward their adoption.

Two-Source Randomness Extractors for Elliptic Curves for Authenticated Key Exchange.
A new construction for a two-sources randomness extractor for elliptic curves defined over a finite field K. The proposed construction can be used in key exchange protocol, design of strong pseudo-random number generators, etc.

The conference was very international, the majority of the participants were from Africa but there were also researchers from USA, Mexico, Canada, China, Japan and Europe.

At the end of this report I have also to mention the kindness of people from the *University Mohammed V* in Rabat and the amazing food we tried during lunches and coffee breaks. Morocco and Rabat are really worthy!
An advice, if you can speak a little bit of French, everything will be easier!