MMC-17
Mathematical Methods for Cryptography

Irene Villa

04-08 September 2017
Svolvær, Norway

The first week of September COINS supported me to attend the workshop *Mathematical Methods for Cryptography*, held in Svolvær, in the archipelago Lofoten in Norway. The event was dedicated to celebrate Prof. *Tor Helleseth*'s 70th birthday, well-known member of Selmer Center, Department of Informatics, University of Bergen.

The workshop was focused on all technical aspects of mathematical methods used in cryptology and related fields such as:

- foundational theory in cryptography,
- design, proposal and analysis of cryptographic primitives,
- coding theory,
- sequences and their application in coding theory and cryptography,
- correlation and transformation of Boolean functions,
- finite fields theory and its application in cryptography.

Full program of the workshop, among with the abstract and the presentation slides of the talks given, can be downloaded from the event web-page (http://people.uib.no/chunlei.li/workshops/lofoten/program.html).

Different topics were covered during the days of the conference, in the following I will describe some of the talks given.

Bart Preneel, from University of Leuven, Belgium, talked about "A perspective on cryptocurrencies". He discussed the principles of distributed currencies, their strengths and weaknesses and gave an overview of cryptographic research challenges related to cryptocurrencies.

Ryan Henry, from Indiana University, USA, gave a talk on "Computing Low-Weight Discrete Logarithms". He analysed the discrete logarithm problem, i.e. given g, h find the element x such that $h = g^x$, when radix-b representation of the exponent sought is know to have 'low weight'.

Claude Carlet, from Univesity of Paris 8, France, presented a work on "Characterizations of differentially uniform functions by the Walsh transform related cyclic difference set-like combinatorial structures". He introduced two notions for Boolean functions, related to the APN property and the Walsh spectrum, and presented his study on the relations between these notions and the known APN functions.

Håvard Raddum, from Simula@UiB, talked about "Representing Integer Multiplication Using Binary Decision Diagrams". The factorization of the RSA modulus $N = pq$ cannot be done efficiently in the classical computational model without the knowledge of one of the two integers p or q. In the talk it was presented a model to factorize N using the Binary Decision Diagrams. Each bit in the unknown factors p and q are treated as variables and, since BDDs can be used to represent systems of Boolean equations, it was shown how to build a BDD that represents the multiplication of p and q consistent with the known bits of N.

Joan Daemen, from Radboud University in Nijmegen,the Netherlands and STMicroelectronics, gave a talk on "Column-parity mixing layers". Mixing layers are an essential ingredient in most modern block ciphers. The speaker studied a generalization of the mixing layer in Keccak-f, the permutation underlying the NIST standard SHA-3 and the authenticated encryption schemes Keyak and Ketje. He investigated their algebraic and diffusion properties and implementation cost.

Many other talks were given during the workshop. Even if many of them were not really focused on my research area, it was very interesting to have a taste of other aspects of Cryptography. It was also useful to see the connections with my work and its possible development.

I am really grateful to COINS that gave me this interesting and useful opportunity!