Mathematical Methods for Cryptography
Reflection report

Nikolay Kaleyski

October 31, 2017

The "Mathematical Methods for Cryptography" (MMC-17) workshop took place between the fourth and eighth of September 2017 in the town of Svolvær in Norway's scenic Lofoten archipelago. The event was held in celebration of the 70th birthday of Professor Tor Helleseth and consequently comprised a number of intriguing talks from the fields of cryptography, mathematics and computer science, given by some of the most prominent researchers in the area and hosted in the conference facilities of the Thon Hotel Lofoten.

As one would expect, the talks (and discussion, in general) encompassed a wide variety of topics related to different aspects of cryptography, and for this reason the remainder of this report will focus mostly on the details of several selected talks. A complete list of all the talks, along with their abstracts and slides (as well as other useful information about the event) can be found on the workshop's web pages at *http://people.uib.no/chunlei.li/workshops/lofoten.*

Aside from the talks themselves, the event provided me with the opportunity to meet a number of people from my own field (including the authors of some of the papers on which my current research is based) as well as from closely related areas, and even to engage in several interesting discussions. Overall, attending the workshop proved to be not only a very productive experience, allowing me to orient myself better in my field and suggesting new ideas and methods of research, but a very pleasant one as well, and I am happy to have had the possibility of taking part in it.

Detailed descriptions of selected talks

"Characterizations of differentially uniform functions by the Walsh transform and related cyclic difference set-like combinatorial structures" - Claude Carlet

Claude Carlet, professor at the University of Paris VIII and a leading authority on the subject of optimal Boolean functions for cryptography, presented his research on the topic of characterizing differentially uniform Boolean functions by their Walsh transform. It is worth recalling that a function F is said to be differentially δ-uniform if all equations of the type

$$F(x) + F(a + x) = b$$

has at most δ solutions for any non-zero a and any b; in particular, 2-uniform functions are called "almost perfect non-linear" (APN) and are cryptographically optimal in the sense that they provide the best possible resistance to the so-called differential attack. The investigation of the properties and construction of such functions is an on-going process, and new characterizations are crucial for progress in this area. In the talk, professor Carlet shows two new characterizations by means of the Walsh transform (note that a number of well-known characterizations of APN functions using the Walsh transform do exist, and are typically very useful for investigating the properties of APN functions; thus, the discovery of additional characterizations is a promising result that may shed more light on the nature of differentially uniform functions) and also introduces two new classes of Boolean functions, viz. componentwise APN functions and componentwise Walsh uniform functions, which are naturally derived from the characterizations and represent particular cases of APN and differentially uniform functions, respectively. Furthermore, some of the properties of these new classes of functions are examined in the talk and certain well-known families of Boolean functions, e.g. the Kasami functions, are classified under them.

My project being related to the study of optimal Boolean functions (and APN functions, in particular), the results and techniques discussed during this talk relate directly to my research, and I am already trying to utilize them in my investigations.

"Code-based post-quantum cryptography" - Jong-Seon No
"Quantum Attacks on Symmetric Crypto" - Gregor Leander

Two talks were given on the topic of quantum computing and its implications for the security of various cryptographic systems and techniques. In essence, a large number of the currently used cryptographic solutions rely on the fact that sufficiently large instances of a given problem are difficult to solve with today's computational technology (for instance, RSA is based on the problem of factoring the product of two large prime numbers; the discrete logarithm problem also underlies a number of popular cryptosystems), but the creation of a quantum computer would allow instances of these problems to be solved (and hence the resulting encryption to be broken) efficiently, so that the cryptosystems in question would be rendered insecure. The investigations in this area then branch into two main directions: how quantum computers can be used to break existing ciphers, and how new encryption methods can be designed which are resistant to such "quantum attacks". Although not directly related to my current research, this topic is nonetheless interesting for me as its implications extend to all areas of cryptography, and also due to the fact that the underlying analysis is based on the computational complexity of certain problems, i.e. is of interest in and of itself and is not restricted to the study of quantum computing.

The talk of professor Jong-Seon No of Seoul National University concerned the so-called "code-based" approach to post-quantum cryptography, i.e. the utilization of certain linear codes for cryptographic purposes; the McEliece cryptosystem (which relies on the problem of decoding a general linear code being NP-hard and impossible to solve efficiently even with the help of a quantum computer) and its practical disadvantages (the large size of the public and private key) as well as various attempts to remedy the latter were discussed at some length; the author then presented his own research, which involved replacing the Goppa code originally used in the cryptosystem by a Reed-Muller code (giving shorter key lengths) while modifying the code (by puncturing and random insertion) so as to overcome the security problems which this would normally introduce.

Conversely, Gregor Leander of the Ruhr-University Bochum presented a quantum algorithm which can be used to break a cipher with key whitening (a popular technique for increasing the key-length of any given cipher) with essentially the same time complexity as for breaking the original cipher (without key whitening). The implication is that key whitening is not an effective means of improving the security of a cipher if quantum computation is involved.

Other talks

Many of the talks touched on topics encountered throughout cryptography in general; to name just a few examples (since otherwise it would be impossible to keep the length of this report reasonable), Kaisa Nyberg (Aalto University) and Igor Semaev (University of Bergen) both talked about various aspects of linear cryptanalysis (which is one of the most frequent attacks employed against cryptographic ciphers and thereby one of the main factors that motivate the investigation of optimal functions). Ryan Henry (Indiana University Bloomington) discussed how the discrete logarithm problem (already mentioned above) can be efficiently solved in certain particular cases, and the practical consequences thereof.