Cost Training School on Symmetric Cryptography and Blockchain

19-23 February, 2018, Torremolinos, Spain

Report for COINS Research School
by Diana Davidova

The winter school on Symmetric Cryptography and Blockchain, co-organized with the COST action IC1306 Cryptography for Secure Digital Interaction, took place in the southernmost region of Spain, Andalusia, in the city Torremolinos (near by Malaga) on 19-23 February 2018.

The topic of the school was "Symmetric Cryptography and Blockchain". There was given lectures on symmetric cryptography and was held discussions on blockchain technologies. The school was oriented not only for Ph.D. students but also for people from security industry. During the lectures was covered all aspects of the topic: from theoretical part to practice. There was presented the classic block cipher design principle as well as some new trends like ciphers with minimal multiplicative complexity, modes of operation for encryption, some generic attacks against modes. In the second part of the school was presented an authenticated encryption mainly from a provable-security perspective, generic composition of authentication and encryption and other. One of the topics discussed during the school was blockchains. Nowadays it is one of the most hot topics and the first example of blockchain, known even by people out of the security and cryptography topics, is bitcoin. All talks during the school were given by famous specialists in their area.

One of the talks was given by *Anne Canteaut from Inria Paris-Rocquencourt research centre, France.* The title of lecture was **"Secure building-blocks against differential and linear attacks"** and it was consists of 5 parts:

- Representations of Sboxes;
- Linear approximations of a Boolean function and Walsh transform;
- Resistance to differential attacks;
- Finding good Sboxes;
- Security criteria for the linear layer.

There was defined basic concepts of a Boolean function and vectorial Boolean function, and their representation by truth tables.Besides the truth table, there are several other representations of Boolean functions which may be more appropriate in some contexts.In coding theory and in cryptography, a very natural representation is the so-called algebraic normal form (ANF), which corresponds to the expression of a Boolean function as a multivariate polynomial.There is an efficient algorithm for computing the ANF of a Boolean function by given truth table. The main idea of linear attack is: use linear relations between the input and output bits of the cipher which hold with probability significantly greater or significantly less than $\frac{1}{2}$.

During the practical part of the school we had many different and interesting exercises. It was a good chance to apply knowledges that we got in theory to solution of practical problems.

I am appreciated a lot to COINS for the opportunity to participate in such interesting and useful event.