# 3 Overview of Talks

## 3.1 On Ciphers that Continuously Access the Non-Volatile Key

*Frederik Armknecht (Universität Mannheim, DE)*


**Joint work of** Frederik Armknecht, Christian Müller, Vasily Mikhalev

Due to the increased use of devices with restricted resources, the community has developed various techniques for designing lightweight ciphers. One approach that is increasingly discussed is to use the key that is stored on the device in non-volatile memory not only for initialization but during the encryption/decryption process as well. This may on the one hand help to save area size, but also may allow for a stronger key involvement and hence higher security.

However, only little is known so far if and to what extend this approach is indeed practical. In this work, we investigate this question. After a discussion on reasonable approaches for storing a key in non-volatile memory, motivated by several commercial products we focus on the case that the key is stored in EEPROM. Here, we highlight existing constraints and derive that some designs are better suited for reducing the area size than others. Based on these findings, we improve an existing design for proposing a new lightweight stream cipher that (i) has a significantly smaller area size than almost all other stream ciphers and (ii) can be efficiently realized using common non-volatile memory techniques. Hence, we see our work as an important step towards putting such designs on a more solid ground and to initiate further discussions on realistic designs.

## 3.2 Another view of the division property

*Anne Canteaut (INRIA – Paris, FR)*


**Joint work of** Anne Canteaut, Christina Boura

A new distinguishing property against block ciphers, called the division property, was introduced by Todo at Eurocrypt 2015. Our work gives a new approach to it by the introduction of the notion of parity sets. First of all, this new notion permits us to formulate and characterize in a simple way the division property of any order. At a second step, we are interested in the way of building distinguishers on a block cipher by considering some further properties of parity sets, generalising the division property. We detail in particular this approach for substitution-permutation networks. To illustrate our method, we provide low-data distinguishers against reduced-round Present. These distinguishers reach a much higher number of rounds than generic distinguishers based on the division property and demonstrate, amongst others, how the distinguishers can be improved when the properties of the linear and the Sbox layer are taken into account.