On the efficiency of code-based block cipher constructions

A. Bogdanov

K.U.Leuven

Block ciphers are central to protecting functionality in security applications. Apart from their vital role for bulk encryption, they are also widely used in the design of hash functions and MAC which provide authenticity. A great deal of recent block ciphers rely on substitution-permutation networks: a construction based on iteratively applying highly nonlinear local maps interlaced with linear diffusion. The latter is often derived from the generator matrices of linear codes. The properties of the codes determine both the security and cost of the resulting designs with respect to such important classes of attacks as differential and linear cryptanalysis. In this talk, we will discuss approaches to formally measuring the efficiency (a trade-off between security and cost) of code-based block cipher designs, introduce several efficiency metrics, and provide a thorough comparative analysis of various code-based constructions with respect to these metrics.