An optimal universal construction of threshold implementation

Enrico Piccione

University of Bergen, Norway

Threshold implementation is a method based on secret sharing to secure the hardware implementation of cryptographic ciphers against differential power analysis (DPA) side-channel attacks. This method was proposed by Nikova, Rechberger, and Rijmen in 2006 to mitigate the leakage caused by glitches. Mathematically, a threshold implementation is a vectorial Boolean function $\mathcal{F}$ with some properties strictly related to another vectorial Boolean function F which is the target function we want to implement. There is a special interest in implementing permutations F over $\mathbb{F}_2^n$ because of their application in SPN ciphers. The need to satisfy those properties make constructing $\mathcal{F}$ a challenging problem especially when F is large in size. Another problem, is to provide threshold implementations with the theoretical minimum number of Boolean shares s, which must be greater or equal than $t+1$ where t is the algebraic degree of F. In this talk, we present the first universal threshold implementation with $t+2$ shares and we discuss some problems related to the construction of threshold implementations with $t+1$ shares.