OPTIMAL FPGA IMPLEMENTATIONS OF VERY LOW-COST COUNTERMEASURE BASED ON ROTATING S-BOXES MASKING COUNTERMEASURE

This talk highlights the low-complexity of the recently proposed Rotating S-Boxes (RSM) by proposing optimal implementations in FPGAs.

Amongst the many existing countermeasures against Side Chanel Attacks (SCA) on symmetrical algorithms, masking is one of the most widespread, thanks to its relatively low overhead, its low performance loss and its robustness against first-order attacks. However, several articles have recently pinpointed the limitations of this countermeasure when matched with variance-based and high-order analyses.

The RSM countermeasure is well adapted to AES and shows the same level in performances as the state-of-the-art, while being less area consuming, and secure against even Variance-based Power Analysis (VPA) and second-order zero-offset CPA.

However this countermeasure needs specific barrelshifters to implement the rotation of S-Boxes.

We present in this paper optimal implementations in FPGAs which still reduce the complexity by keeping a high level of robustness. A security evaluation is also presented with different parameters like the mask and architecture types.