# Area-efficient fault-tolerant architectures exploiting masking scheme randomness

Vojtech Miskovsky, Hana Kubatova, Martin Novotny
Czech Technical University in Prague

### Abstract

Electronic systems become more and more important part of everyday life including safety-critical spheres like transportation or even medical devices. These systems need to fulfill strict dependability properties. To ensure correct operation of such devices, we need to make them fault-tolerant. This is usually achieved using common redundancy schemes like triple-modular redundancy (TMR). These schemes are simple to implement, but introduce high overhead. In case of TMR, we need to replicate the design three times and place majority voters on the outputs. Since these systems are usually connected to some network, their activity and communication should be encrypted. Nevertheless, side-channel analysis pose a threat even to modern cryptographical algorithms. Luckily, many side-channel countermeasures based on hiding or masking exist to protect the device against such an attack. As these countermeasures can introduce very high area and/or power overhead, the total resources of a SCA-protected and fault-tolerant cryptographical module can be unbearable. In our work, we deal with this issue and we present area-efficient fault-tolerant schemes exploiting randomness introduced in masking-based SCA countermeasure. Using our approach, it is for example possible to achieve properties similar to TMR (tolerance to single module failure) using only two redundant modules.