# Embedded Systems for IT Security Applications: Properties and Design Considerations

Sorin Alexander Huss

CASED Research Center for IT Security
Darmstadt, Germany

## Abstract

Embedded systems aimed for applications in the IT security domain are characterized by specific needs in terms of computing power. The high computational loads stem both from algorithms, which have to address different symmetric and especially asymmetric encryption schemes such as AES, RSA, ECC and PBC, and from associated key size values ranging from 100's to several 1000's bits.

The presentation details specific architectural considerations of reconfigurable System-on-Chip implementations aimed to deal with high computational loads. Multiple data paths with pipelining, distributed memory blocks and multiple processor/coprocessor schemes are presented and demonstrated for several application examples.
The design flow for such specific architectures will be addressed by means of a dedicated high-level synthesis tool, which is based on genetic algorithms for the solution of the underlying allocation and scheduling problems.

The talk concludes by addressing novel challenges stemming from requirements on quantum computing resistant encryption modules.

Duration: 45 min