Side Channel Attack Protection for FPGA-based Cryptographic Implementations

As embedded systems are getting more and more networked, security has become an important issue.

In order to ensure that confidential information is only accessible to those authorized to read it, cryptographic algorithms are deployed. For implementing such cryptographic algorithms, FPGAs represent an efficient platform. In symmetric methods, such as e.g. AES, the data is encrypted or decrypted using a secret key. This key must be present in the embedded system. However, this can be extracted by a “poor” implementation using side channel attacks, such as analyzing the power consumption.

In this work, protection measures against power and electromagnetic radiation side channel attacks should be developed, which use the FPGA feature of partial dynamic reconfiguration.

Supervisor:
Daniel Ziener (daniel.ziener@tu-ilmenau.de)