Protection of FPGA-based Cryptographic Implementations from Fault Injection Attacks

Field programmable gate arrays (FPGAs) provide an efficient platform for cryptographic hardware implementations with many advantages. However, any safety-critical circuit implemented on an FPGA must be protected against fault injection attacks. On this kind of attacks, the attacker disturbs the cryptographic component at defined times during the operation in such a way that information about the secret key can be gathered by the extent and type of the error. The threat potential of these fault injection attacks is enormous. Depending on the cryptographic procedure, a single fault can completely compromise the security of the cryptographic implementation.

In this work, fault injection attacks on FPGA-based cryptographic implementations and their countermeasures should be investigated. In particular, it should be analyzed whether encryption of the configuration offers sufficient protection against such attacks.

Prerequisites:	Good knowledge in FPGA design
Type of Work:	Theory (30%), Conception (30%), Implementation (40%)
Supervisor:	Daniel Ziener (d.m.ziener@utwente.nl)