FPGA-based Implementation Attacks with GIAnT

David Oswald
Ruhr-University Bochum, Germany

Abstract

Fault injection is a technique to attack physical implementations of mathematically secure ciphers. Introducing our FPGA-based open-source fault injection platform GIAnT, we enable performing corresponding attacks - that are mostly executed by smartcard evaluation labs using sophisticated equipment - for a wide audience at a low cost. Illustrating the capabilities of GIAnT, we analyze the vulnerability of two popular 8-bit microcontrollers towards fault injection based on voltage variations. The proposed techniques are not restricted to the analyzed example devices, but generally applicable to many other embedded devices.