Differential power analysis attack on implementation of AES algorithm on Xilinx platform

Ondrej Semrad
FIT CTU
Thakurova 9, 160 00 Prague 6, Czech Republic

semraond@fit.cvut.cz

Keywords. Differential Power Analysis, DPA, Security, Safety, FPGA, AES, Rjindael, Xilinx

Abstract

We explored the possibilities of application of Differential Power Analysis (DPA) on the implementation of AES algorithm on the FPGA Spartan-3E by Xilinx. We created two different hardware implementations of the AES cipher in VHDL language, a script implementing the DPA method in the Mathematica software and a wrapper implementing the communication between an AES module and a computer using a serial line. We inserted eight different versions of AES cipher inside the wrapper – five versions with safety measures and three basic versions without any safety measures. We compared the resistance of basic variant with the fault tolerant ones by computing the minimal number of power traces needed for breaking the correct key for each variant. We discovered that the safety measures (hardware redundacy, time redundancy and information redundancy) had minimal influence on the resistance against DPA.

Acknowledgment

Dr.-Ing. Martin Novotny