Side Channel Attack on AES Implementation in Altera Platform

Jan Riha
Faculty of information technology, CTU Prague

rihaja11@fit.cvut.cz

Keywords. differential power analysis, DPA, CPA, AES, Rijndael, FPGA, fault-tolerance, spatial redundancy, time redundancy, information redundancy, Altera, attack-resistance

Abstract

Aim of this work is to compare influence of fault-folerance techniques on differential power-analysis (DPA) resistance of AES cipher implemented in Altera FPGA. After attacking simple variant, I attacked fault-tolerant variants of the cipher and compared results with the simple variant. From the comparison follows that the use of informational redundancy at SubBytes operation, spatial and time redundancy at both round and algorithm level had minimal influence on resistance against DPA, as the number of power traces necessary to obtain the key had not changed significantly.

Acknowledgment

I would like to show my gratitude to Dr.-Ing. Martin Novotny for coming up with this topic and also for his help.