Influence of Fault Tolerant Design Techniques on Resistance against Differential Power Analysis

Vojtěch Miškovský
Czech Technical University in Prague
Faculty of Information Technology
Department of Digital Design

Abstract

The security is becoming more and more important issue these days, but we still should consider reliability. When we design a cryptographic device e.g. for some mission-critical or another reliability demanding system, we need to make the device not only attack resistant, but also fault tolerant.

In context of the digital design we usually talk about resistance against side channel attacks, because these are not based on cryptographic properties of the cipher, but on properties of its physical implementation. For example power attacks use powertrace of the device to reveal some secret information about the device, usually a cipher key during an encryption.

We know many digital design techniques used to secure the device against power attacks with some area and time overhead. But what happens, if we want to make the device also fault tolerant? Many fault tolerant architectures are based on some kind of redundancy. This redundancy introduces large area and also power consumption overhead. But does this overhead have any influence on the attack resistance? And what about the overhead? Isn't there any way to decrease the overhead by some combined attack resistant and fault tolerant architecture? We try to answer these questions in our research.

We compared vulnerability to differential power analysis of a simple AES cipher implementation and its multiple fault tolerant variants implemented in FPGA. Results of this comparison will be presented.

When we were experimenting with differential power analysis against FPGAs we found out that computation requirements of the attack demand an implementation that is more efficient than scripts in Wolfram Mathematica or MATLAB. We decided to program a high performance and numerically stable application for this purpose. This application and its properties will also be presented.

Acknowledgment

This research has been partially supported by the grant GA16-05179S of the Czech Grant Agency, "Fault-Tolerant and Attack-Resistant Architectures Based on Programmable Devices: Research of Interplay and Common Features" (2016-2018) and CTU project SGS17/213/OHK3/3T/18.