Side channel analysis of cryptographic algorithms implementations

Lukáš Mazur
Faculty of Information Technology, Czech Technical University in Prague
Thákurova 9, 160 00 Prague, Czech Republic

mazurluk@fit.cvut.cz

Keywords. Differential Power Analysis, Side Channel Attacks, Advanced Encryption Standard, FPGA, Smart Card, Correlation Analysis.

Abstract

We explored the possibilities of the Differential Power Analysis (DPA) on the Field Programmable Gate Array (FPGA). We have modified the application for measuring a power consumption, created scripts for performing DPA, and created different implementations of AES algorithm for FPGA. Developed scripts and applications for DPA were verified against AES implementation for smart cards. Once those applications successfully broke the implementation for smart cards, we continued with the application of DPA against AES implementation for an FPGA board. DPA against FPGA was performed in six different configurations. Those configurations differed in AES implementation for FPGA, in board configuration, in oscilloscope setup, and in method of the attack. We found variants that could be successfully broken. We found out that an oscilloscope and measuring environment setups has major impact on the feasibility of the DPA on FPGA. The implementation is less important for the success of the attack. The most important aspect of the implementation was the clock frequency. We have also found out that using different power sources and removing capacitors on the FPGA board have significant impact on the feasibility of the DPA.