Electromagnetic Fault Injection

Platform for Attack Generation

Graduate

Eric Walser

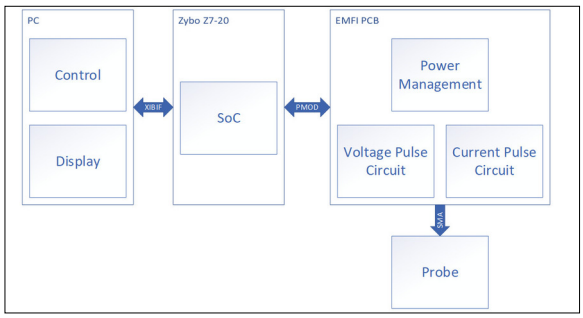
Flavio Grepper

Introduction: By performing so called side-channel attacks against cryptosystems, an attacker aims to extract critical information from these systems. Electromagnetic fault injection (EMFI) is such a method to trigger a misbehaviour on the target chip. An electromagnetic pulse (EMP) with a fast-changing magnetic field induces a voltage in the chip and causes malfunctions. The aim of this bachelor thesis is to develop a platform for generating such EMPs. It should help to gain a better understanding of EMP side-channel attacks.

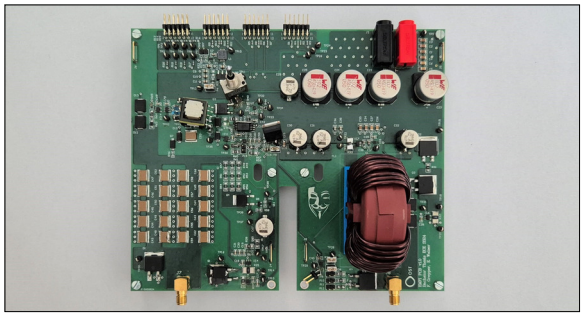
Approach: A literature study revealed two approaches for EMFI. In the voltage pulse method, a generated high voltage is applied to an injection probe. For the second method a storage coil is loaded with a high current. As soon as the desired current is reached, a switch forces the current to flow through the injection probe. Both methods were implemented on a two-layer PCB after the concepts had been analysed in simulations. In parallel, VHDL and Python code was designed. The hardware control is implemented in VHDL. Python helps with automatic testing, debugging and takes care of the communication between user application and hardware. Additionally, a "small", "medium" and "big" injection probe were made. The setup was then used for attacking an Artix-7 FPGA with two different designs: ring oscillators for frequency disturbance and counters for logic faults.

Conclusion: The designed attack platform can generate voltage pulses of up to 1kV. With the created injection probes and voltage pulses of 100V, it is possible to disrupt counters, by disturbing the timings of the digital logic. Additionally, the misbehaviour of ring oscillators is already reproducible with 50V. Depending on the used voltage, type and position of the injection probe, the frequency of ~80MHz changes more than 50%. Although EMFI works with the current pulse circuit, the loading of the storage coil still has an unclear behaviour and needs further investigation. The platform proofs the concept of EMFI and allows to attack cryptographic implementations. Finally, improvements and further steps for a next potential PCB iteration were defined.

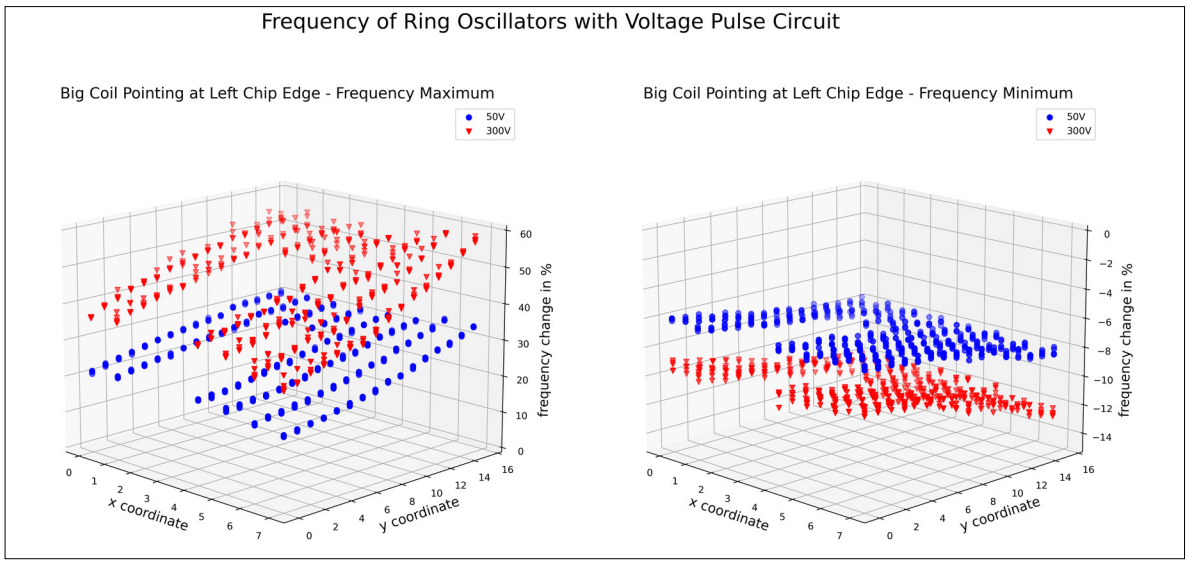
Overview of the created platform for attack generation.
Own presentment



The developed EMFI PCB with the voltage pulse circuit on the left side and the current pulse circuit on the right side.
Own presentment



Frequency change of ring oscillators on an Artix-7 FPGA due to EMFI with the biggest hand made coil at 50V & 300V.
Own presentment



Advisors
Prof. Dr. Paul Zbinden, Lukas Leuenberger

Co-Examiner
Robert Reutemann, Miromico AG, Zürich, ZH

Subject Area
Microelectronics

Project Partner
IMES Institut für Mikroelektronik, Embedded Systems und Sensorik, OST - Ostschweizer Fachhochschule, Rapperswil, SG