Bachelor’s/Master’s Thesis

“Development & Implementation of Hardware Trojan Detection Techniques for IoT Devices”

For the maximum deployment and trust building of users, IoT devices must be secure enough both at hardware and software level. Malicious modifications or insertions called Trojans, could be made possible by untrusted vendors or foundries at any stage of the IC development cycle.

Problem:
An intelligent adversary can add a Trojan circuit that only activates itself under certain circumstances and thus remains undetectable in the test phase. For the detection of such Trojans, three major techniques can be applied.
1. Reverse Engineering
2. Functional Testing
3. Side Channel Analysis

Side channel signal analysis due to its non-destructive nature can be useful to detect Trojans without its activation by measuring the parameters like Power, Temperature, Current or Delay.

Goals:
This thesis aims at development of Trojan Detection Techniques through side channels on the Trojan benchmarks available at: www.trust-hub.org. Proposed techniques can be implemented and evaluated on our Xilinx Virtex-7 FPGA platform by inserting benchmark Trojans in FPGA using VHDL/Verilog. Master’s students will be required to develop a novel methodology for high sensitivity Trojan detection.

Required Knowledge:
- Computer Architecture, VHDL/Verilog

Helpful knowledge:
- Hardware Security Threats
- Design and Profiling tools (e.g. Xilinx Primetime-PX)

You will learn about:
- IoT Security
- Trojan Insertion
- Trojan Detection Techniques

Supervisor:
M.Sc. Qazi Arbab, ces.itec.kit.edu/~ahmed
Email: qazi.ahmed@kit.edu