FPGA-based Fault Simulation

Motivation
Current asymmetric cryptography is safe from a mathematical standpoint, but is vulnerable in real-world applications. A very powerful kind of attacks are fault attacks (supply glitch, laser beam). The goal of this project is to find vulnerabilities of an existing elliptic curve design (given in VHDL) by using a fault simulator.

Project description

Goals
• FPGA-based fault simulator
• Add countermeasures to ECC design (for master thesis only)

Tasks
• Literature research
• Investigate the existing IAIK FPGA designflow
• Understand the basics about the elliptic curve reference design
• Build fault simulation environment
  – Design under test modifications
  – Fault case generation
  – Design under test input generation
  – Test automation

Literature
  - www.xilinx.com

Deliverables
- Project files (.zip, cleaned)
- Documentation (inline)
- Readme (getting started)
- Presentation (10.ppt slides)

Project schedule
- Start Immediately
- Month 1 Reading, planning, preparing
- Month 2 FPGA programming
- Month 3 Final deliverables

Master Project
Studies: ☒ INF ☒ SEW ☒ TEL

Prerequisites
- Hardware modeling (VHDL / Verilog)
- Application flow scripting

Advisor / contact
Erich.Wenger@iaik.tugraz.at