A Novel Experimental FPGA Hardware Platform for Power Analysis Attacks

Michal Varchola: Technical University of Kosice, Slovakia, +421903582477, michal@varchola.com
Milos Drutarovsky: Technical University of Kosice, Slovakia, milos.drutarovsky@tuke.sk
Marek Repka: Slovak University of Technology in Bratislava, Slovakia, marek.repka@stuba.sk

Abstract: We are introducing a novel experimental platform (Fig. 1) for measuring power consumption of FPGAs (namely the Altera Cyclone III) during experimental power analysis attacks. Our system provides the following features: A) both classic and new measurement points (Fig. 2, Fig. 3): current flow from a linear regulator to the FPGA; current flow from the power supply to a linear regulator; current flow from a decoupling capacitor to the FPGA; the voltage on the decoupling capacitor. B) an EMI shield which protects the entire DISIPA board against electromagnetic pollution. C) Strong Murata filters are assembled on a power line in order to minimize noise from the power supply (as well as leaks from the board). The FPGA + measurement points circuitry have their own chamber in the shield. All: linear regulators + filters, configuration circuitry, input/output circuitry, and the main Murata filter have separate chambers as well. We expect that the described improvements will enhance signal-to-noise ratio of the leakage, or in other words will reduce the number of traces needed for a successful DPA attack. We want to get as clean leakage signal as possible in order to assess the strength of particular countermeasures. We are curious, if simple (but efficient) EMI shielding, or the usage of another measurement point causes otherwise secure DPA countermeasure to be inadequate.

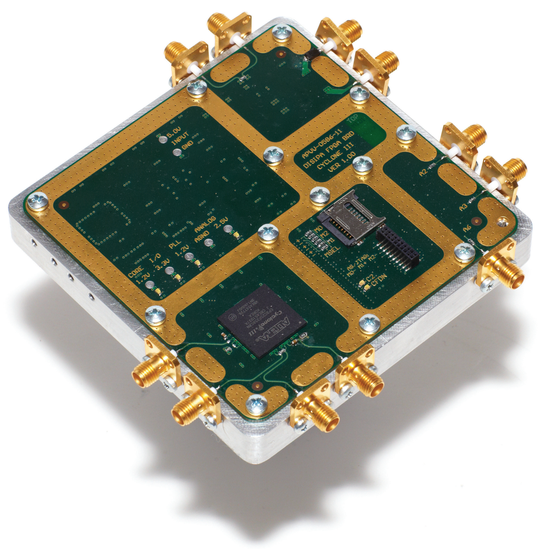

Fig 1. The DISIPA Board

Main Advantages:

- 4 Sensing Points Available
  - current flow from external supply **(1)**
  - current flow to FPGA's core **(2)**
  - voltage at FPGA's core **(3)**
  - current flow via decoupling capacitor **(4)**
- Electromagnetic Shield
  - eliminates atmospheric noise

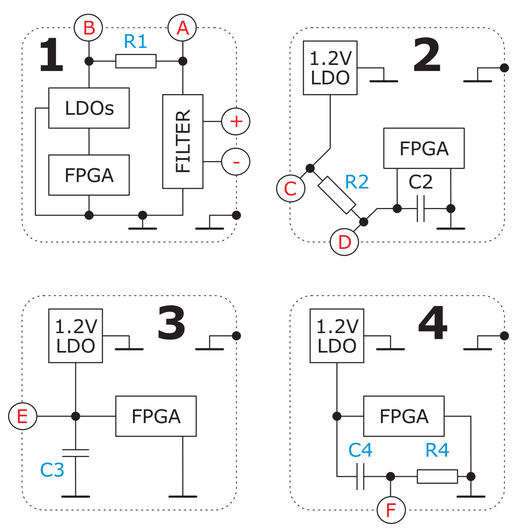

Fig 2. Measuring points in the DISIPA Board

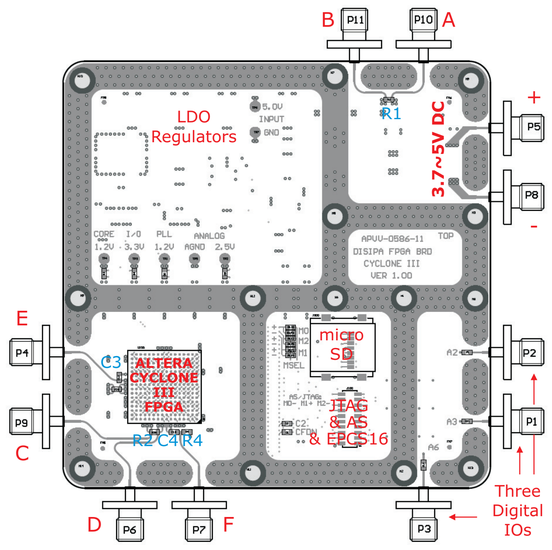

Fig 3. DISIPA board drawing

Up to now, we have found that the selection of measurement points matters. The voltage drop on a series measurement resistor is definitely not the best choice. When selecting proper measurement points (Fig. 4) and proper oscilloscope interconnections, we needed only 75 traces (Fig. 5) to attack a single AES SBOX design (for any 8-bit fragment of key), or 900 traces (Fig. 6) to attack one of the 16 AES SBOXes operating in parallel (for any 8-bit fragment of key). Moreover, despite the strong filtration of the power line, we were able to perform successful DPA attacks by acquiring traces on the power cord. The distance between the board and a measurement point was approximately 50 centimeters. We used a cascade of two 35 dB amplifiers (70 dB in total), an Agilent DSO9404A oscilloscope and enhanced pre-processing of acquired traces based on an investigation of clock-frequency harmonics (Fig. 7). Thus, we needed 500k traces to perform a successful attack on a single SBOX (Fig. 8). An interesting fact is that the otherwise narrow correlation peak (when measuring directly on the FPGA) was spread out intime for at least 100 clock cycles. The amplitude of clock-frequency harmonics was just several tens of nano-volts.

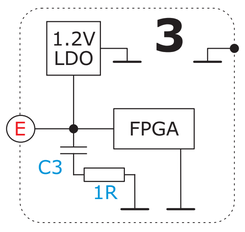

Fig 4. Modified measuring point 3

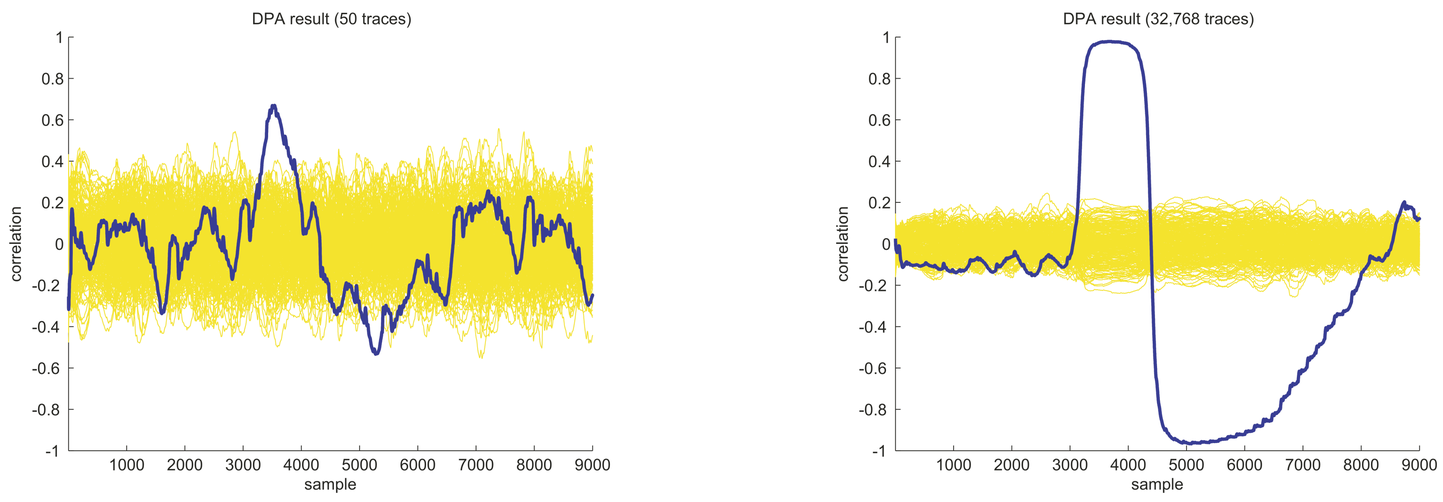

Fig 5. DPA attack against 1 AES SBOX using modified measuring point 3 and +15 dB wideband amplifier

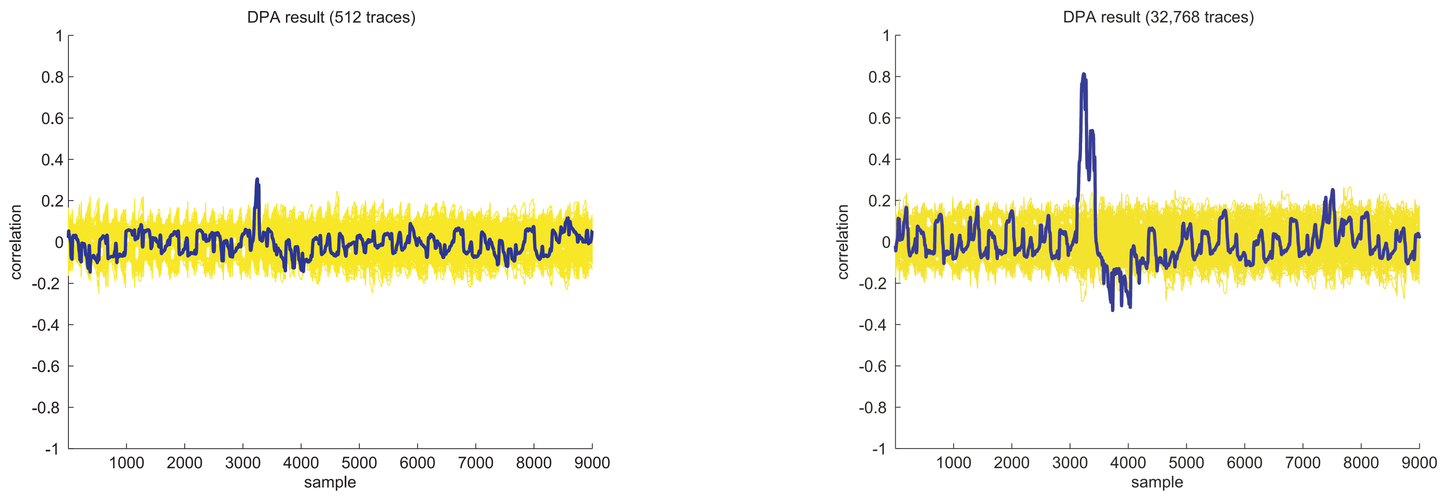

Fig 6. DPA attack against 16 parallel AES SBOXes using modified measuring point 3 and +33 dB wideband amplifier

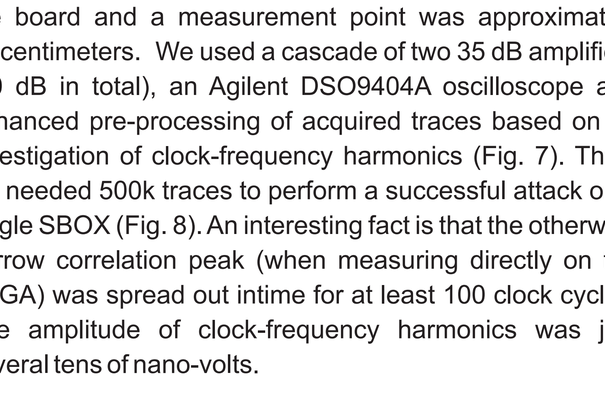

Fig 7. Measurement on the power cord setup

Fig 8. DPA attack against 1 AES SBOX by acquiring traces on the power cord and using +70 dB wideband amplifier

The Altera Cycolne III FPGA board was developed and sponsored by the DISIPA (DIgital SIgnature Power Analysis) project. The project consortium consists of the Technical University of Kosice (TUKE), the Slovak University of Technology in Bratislava (STU) and the Micronic corp. The project is supported by the Slovak Research and Development Agency (APVV); project code: APVV-0586-11; acronym: DISIPA.