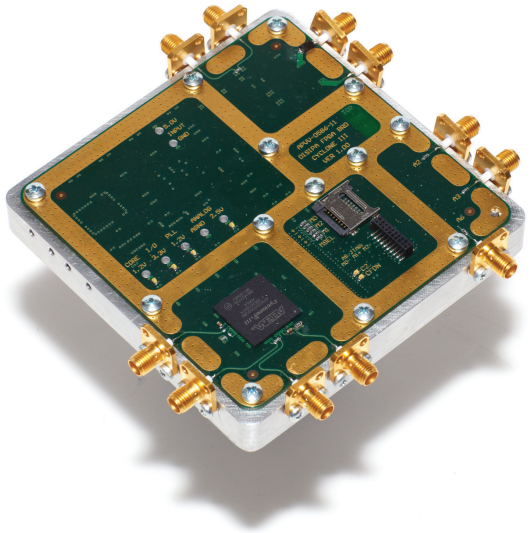
DISIPA

A Novel Power Analysis Hardware Platform

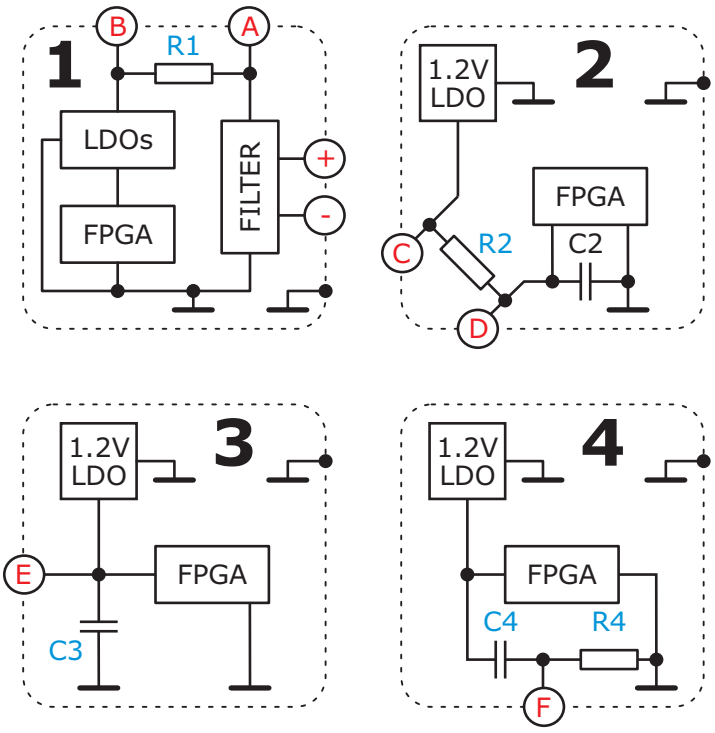


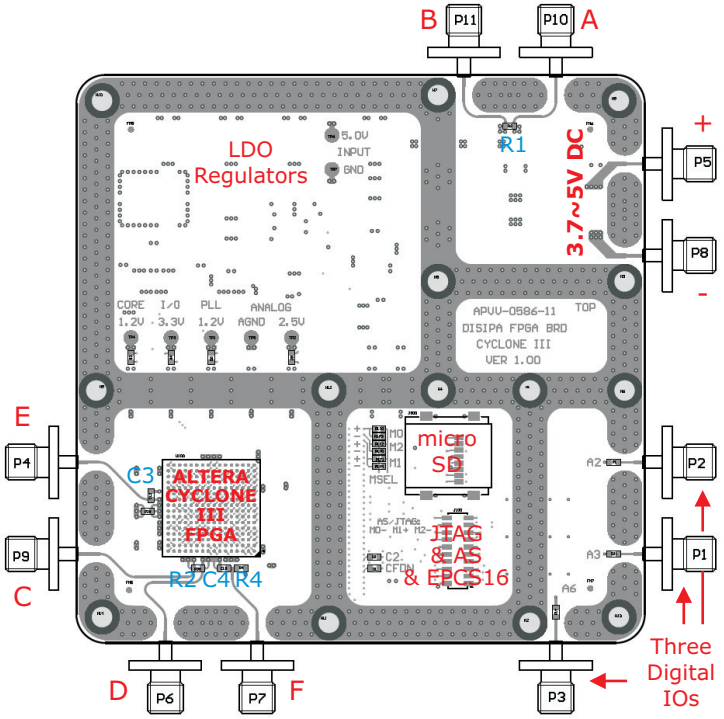
Main Advantages:

- 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

We introduce a novel platform for measuring power consumption of FPGAs towards performing power analysis attacks. The Altera Cycolne III FPGA board was developed and sponsored by the DISIPA (DIgital SIgnature Power Analysis) project. Our board provides following features: I) both classic and new measuring points: the current flow from linear regulator to FPGA **(2)**; the current flow from power supply to linear regulator **(1)**; the current flow from decoupling capacitor to FPGA **(4)**; the voltage at decoupling capacitor **(3)**. II) EMI shield which protects entire DISIPA board against electromagnetic pollution. The FPGA and measuring points circuitry have their own chamber in the shield. We expect that described improvements will enhance the signal-to-noise ratio, or in other words will reduce number of traces needed for successful DPA attack. We want to get as clean signal as possible in order to assess the strength of particular countermeasures. We are curious if a simple (but efficient) EMI shielding or using of another measuring point causes otherwise secure DPA countermeasure to be inadequate. Our DISIPA project mainly focuses at ECC based digital signatures, however hardware platform is not limited in the terms of used cryptographic algorithm. We will present physical hardware platform and preliminary results at the Reconfig'13 Demo Night. The project consortium consists of Technical University of Kosice (TUKE), Slovak University of Technology in Bratislava (STU) and the Micronic corp. The project is supported by Slovak Research and Development Agency (APVV); project code:APVV-0586-11; acronym:DISIPA



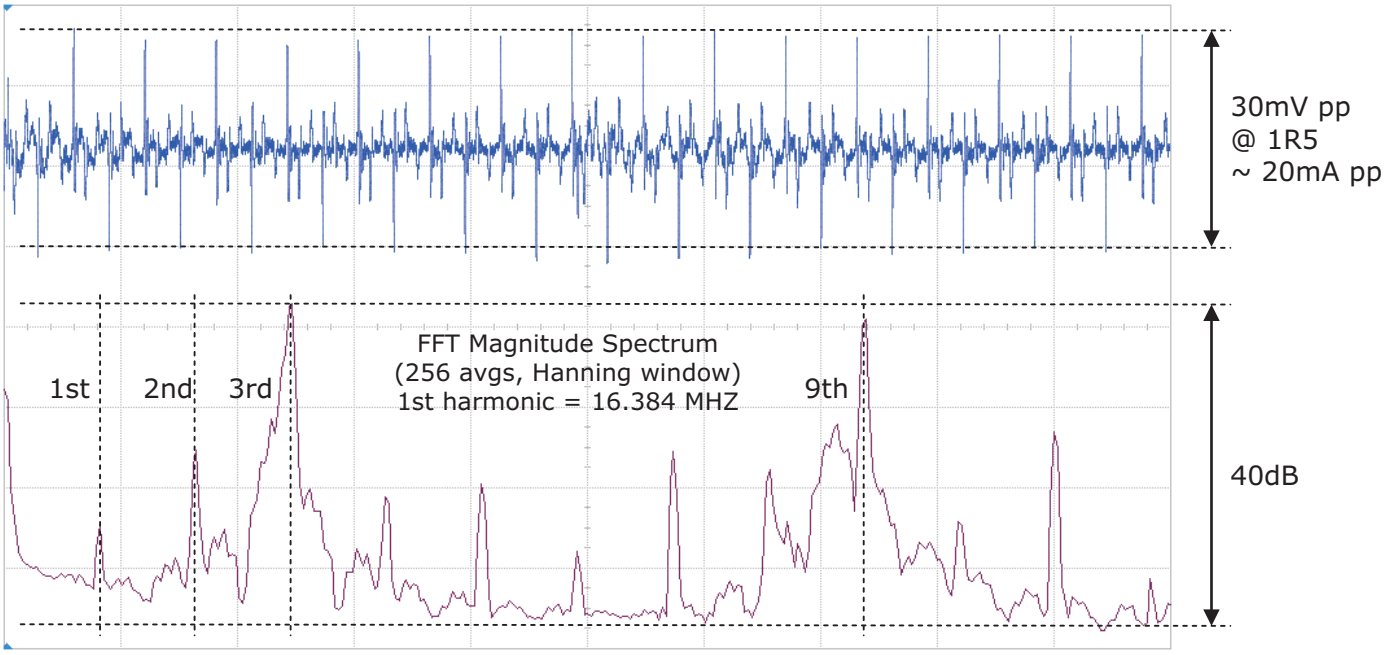


STU FEI

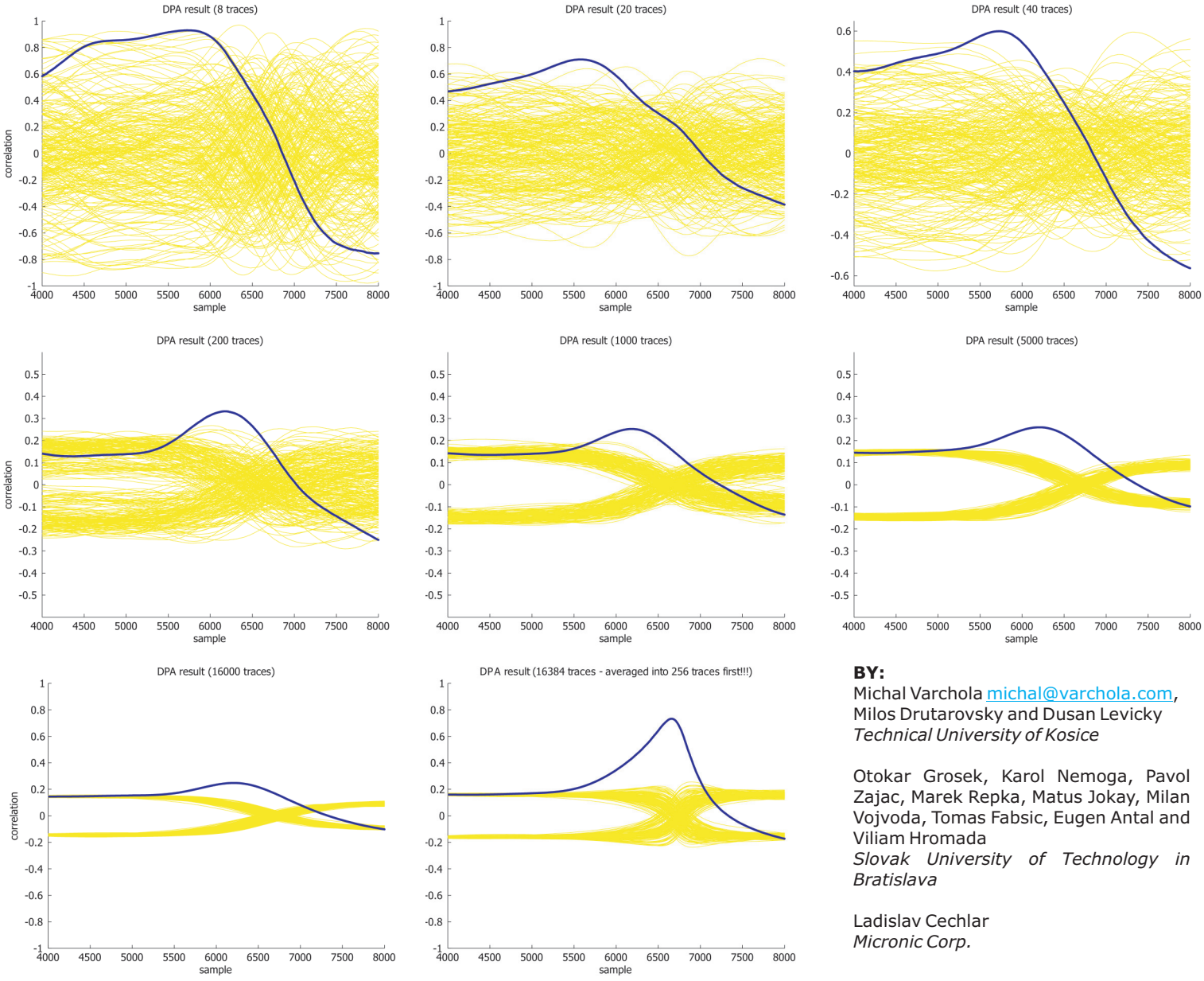
MICRONIC

SLOVAK RESEARCH AND DEVELOPMENT AGENCY

An Example - Attacking the AES S-BOX Result in Stored Register



Measurement using sensing point **(4)** - current via decoupling capacitor, measured by Agilent DSO9404A oscilloscope. DISIPA board was connected directly to oscilloscope by the PASTERNACK coaxial cable.



BY:
Michal Varchola michal@varchola.com,
Milos Drutarovsky and Dusan Levicky
Technical University of Kosice

Otokar Grosek, Karol Nemoga, Pavol Zajac, Marek Repka, Matus Jokay, Milan Vojvoda, Tomas Fabsic, Eugen Antal and Viliam Hromada
Slovak University of Technology in Bratislava

Ladislav Cechlar
Micronic Corp.

DPA Attack results with various number of traces. Blue line represents the correct hypothesis. All traces were pre-processed by demodulation and filtering. Traces in the last figure were averaged prior to applying the pre-processing and attack algorithms.