Differential Power Analysis under Constrained Budget: Low Cost Education of Hackers

Filip Štěpánek Jiří Buček Martin Novotný

Faculty of Information Technology
Czech Technical University in Prague

Outline

Previous form of education

Procedure:

- Traces measured/given by the tutor (available oscilloscopes $25,000 each)
- Students only analyzed given traces

Disadvantages:

- No hands-on experience
  - No work with oscilloscope
  - No acquiring the traces
- No connection between the theory and the practice
- Traces were used as black-box

New proposed form of education

Procedure:

- Students implement the cipher
- *Students measure the power-traces themselves*
- Students analyze measured traces using the algebraic system

Problem:

- Is it feasible with constrained budget?
  $\Rightarrow$ is there a cheap oscilloscope with sufficient power?

Candidates

Figure: Agilent DSO-X3104A, USB transfer speed 2060 [kSa/s]

Figure: Hameg HMO1024, USB transfer speed 77 [kSa/s]

Figure: GW Instek GDS1152A, USB transfer speed 67 [kSa/s]

Figure: Tektronix MSO2024, USB transfer speed 312 [kSa/s]

Memory & Transfer speed

All oscilloscopes have sufficient memory of $\geq$ 2 MSa.
(measurement using Picoscope 5204 as reference)

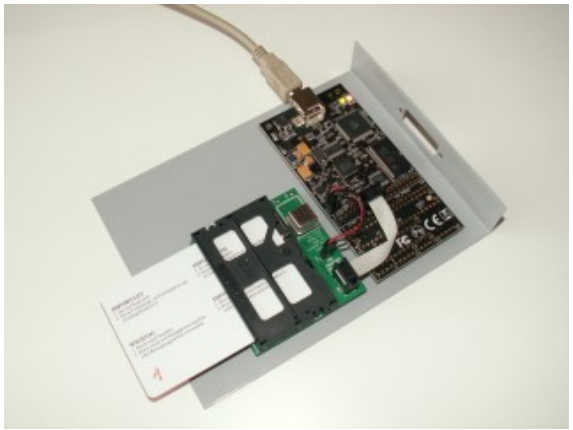
Tested model (alphabetical order)	**USB speed [kSa/s]**	**min. time to transfer 500 traces [minutes]**
Agilent DSO-X3104A	2060	1.5
GW Instek GDS1152A	67	46
Hameg HMO1024	77	40
Tektronix MSO2024	312	9.9

Table: Data transfer speed of tested oscilloscopes.

Transfer speed not mentioned in the datasheets!!!

Other equipment

- AVR smart card



- Card reader

- Smart cards programmer
  - AVR Dragon
  - Smart card interface
- Custom interface board
  - No need to modify the card reader
  - Power and trigger signals

Measuring procedure

- Smart card:
  - Prepared firmware
  - T=1 protocol
  - Students insert their implementation of the chosen cipher
- Oscilloscope/card reader
  - Finding of the desired cycle
  - Automated measurement
  - Data ready for analysis

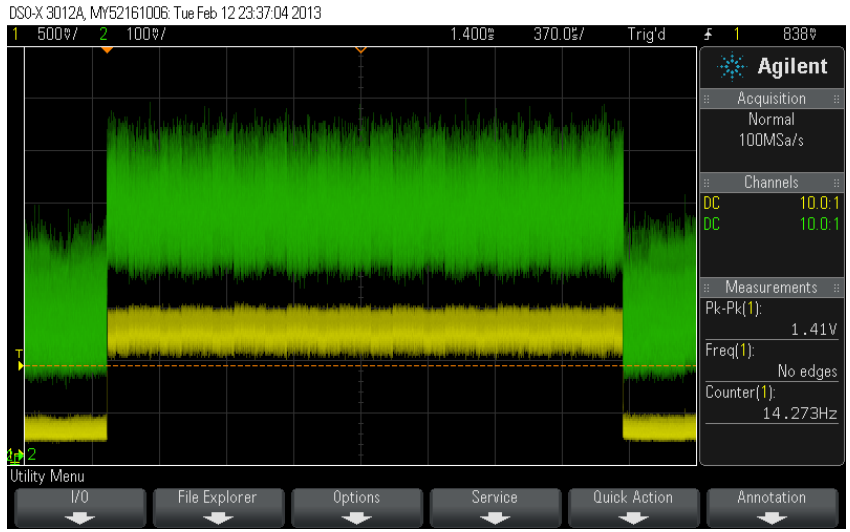


Figure: AES measurement

Summary

- Low cost
  ($2,300 per work station)
- Transfer speed of the oscilloscopes not mentioned in the datasheets
- Efficient DPA education
  - Focus on cipher implementation
  - Hands-on oscilloscope experience
  - 100% success

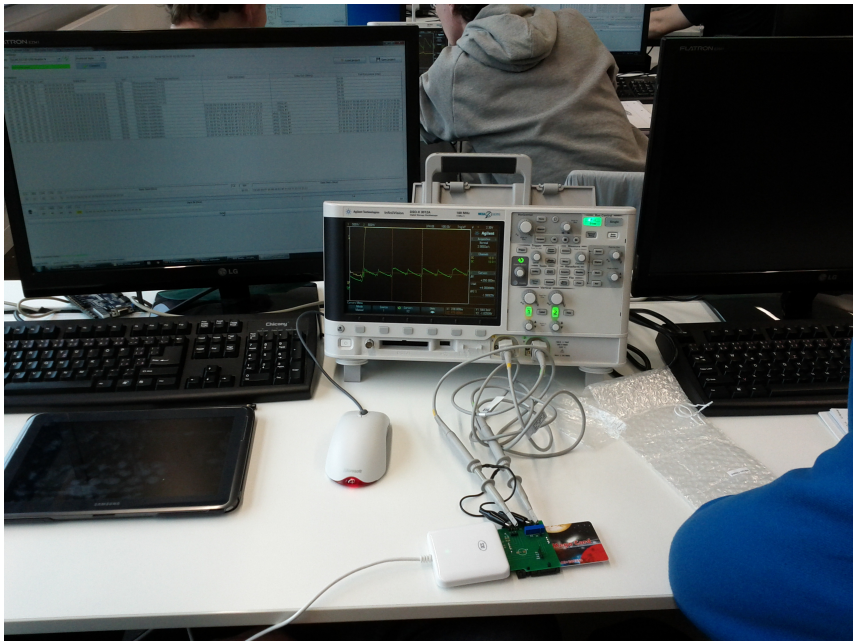


Figure: Laboratory sessions