Automated experimental setup for EM cartography to enhance EM attacks

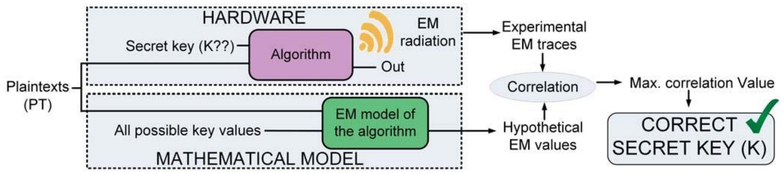
Erica Tena-Sánchez, Alejandro Casado-Galán, Virginia Zúñiga-González,
F. Eugenio Potestad-Ordóñez and Antonio J. Acosta

IMSE-CNM Instituto de Microelectrónica de Sevilla
CSIC Consejo Superior de Investigaciones Científicas
Universidad de Sevilla

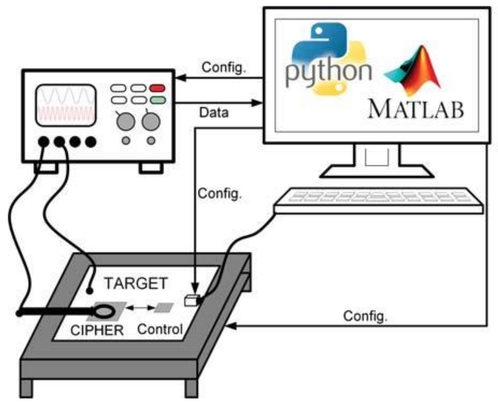
Abstract

Side-channel attacks are a real threat, exploiting and revealing the secret data stored in cryptographic devices. All **ElectroMagnetic (EM) attacks** analyze the relation between the EM radiation and the data being processed. A critical point is the **EM probe** positioning.
An automated experimental setup for **EM cartography** is described to enhance EM attacks and to help hardware designers to detect information leakage flaws

Example: Correlation EM Attacks

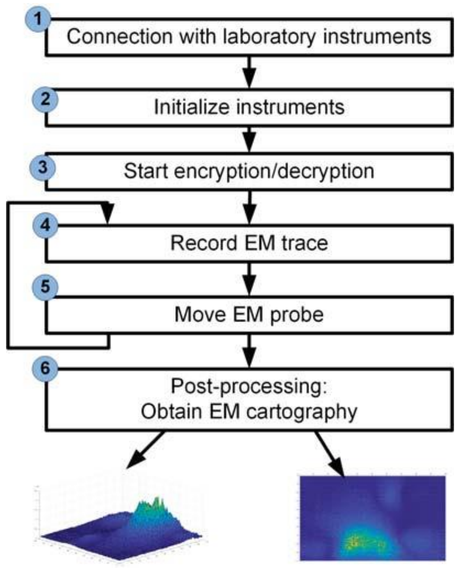


I.- Measure EM radiation in encryption process
II.- Compare to a mathematical model of the algorithm
III.- Analyze the correlation between both
IV.- Extract the secret key



Target device: FPGA with AES encryption algorithm in a non-stop ciphering operation mode

Automated Cartography Steps – MATLAB controlled



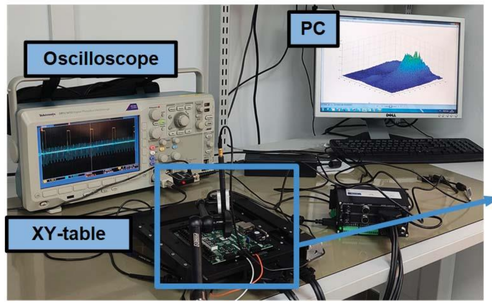
OSCILLOSCOPE:
Tektronik DPO3032

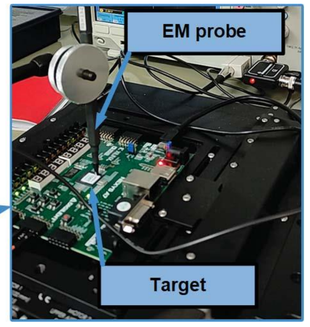
XY-TABLE:
ZABER ASR100B120B

FPGA:
Xilinx Artix-7 on a Nexys4 DDR board

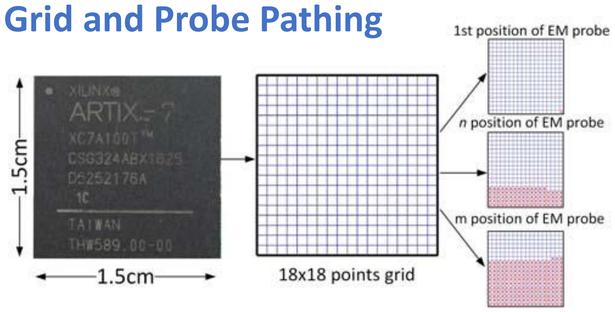
PROBE:
Rohde&Schwarz

PC: Intel Core2 Quad Q6600 - 4GB RAM, Matlab 2018a



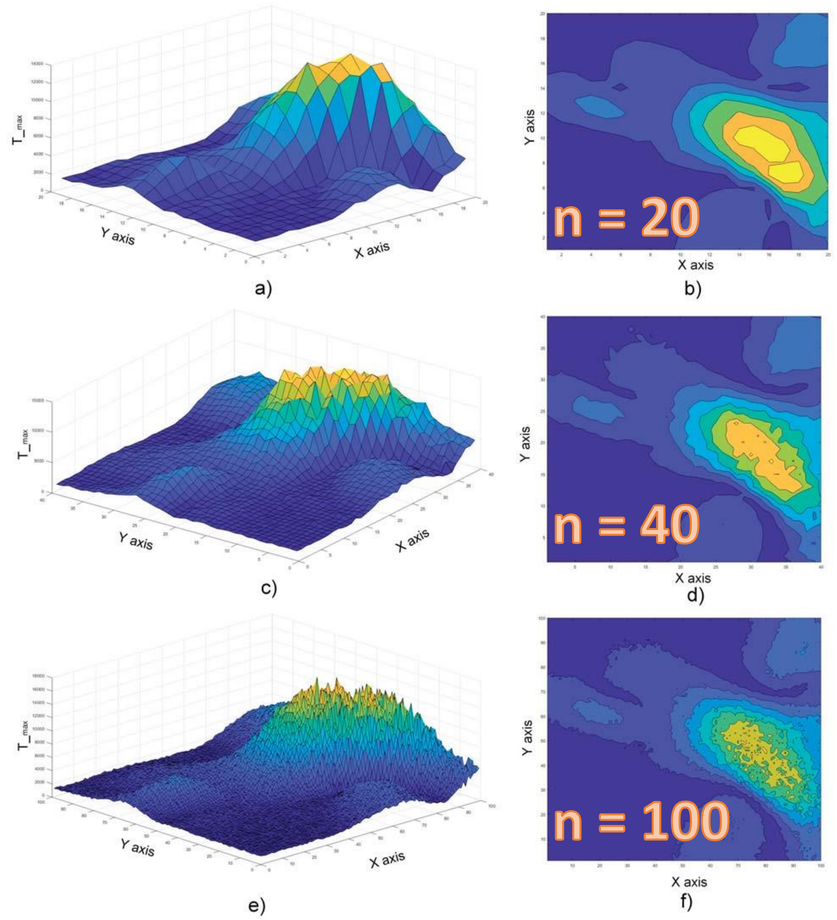


Point Grid and Probe Pathing



After an n-resolution grid is programmed, the probe moves to every of these points collecting the EM emission. The probe path can be also configured

Electromagnetic Maps - Resolution vs Time



Resolution (n)	5	10	20	40	100
# of points	25	100	400	1600	10000
Time (s)	14.28	48.16	170.86	604.32	3643.00

Conclusions

A critical step for a successful EM attack is the probe automated positioning and precise EM cartography generation setup
An experimental Matlab-controlled EM cartography has been generated over an **AES** implementation in a **Xilinx Artix-7 FPGA,** requiring a **PC**, **oscilloscope**, **EM probe**, and **XY-table**
The **number of points** for EM captures is an important cost metric

This work has been funded by project SCAROT 1380823-US/JUNTA/FEDER, UE. Thanks to SPIRS Project with Grant Agreement No. 952622 under the European Union's Horizon 2020 programme and Grant PID2020-116664RB-I00 funded by MCIN/AEI/10.13039/501100011033.