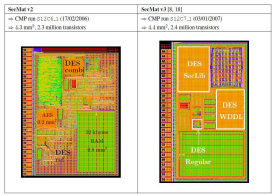
TELECOM ParisTech
Contact: jean-luc.danger@telecom-paristech.fr
http://www.telecom-paristech.fr/

SPACES
Security evaluation of Physically Attacked Cryptoprocessors in Embedded Systems
https://spaces.enst.fr/spaces

Télécom ParisTech : VLSI Research and Contributions

Télécom Paristech, Research on security of embedded systems

Attack Understanding
- DPA contests (versions 1, 2, 3, 4)
- DPA, CPA, MIA, template, stochastic



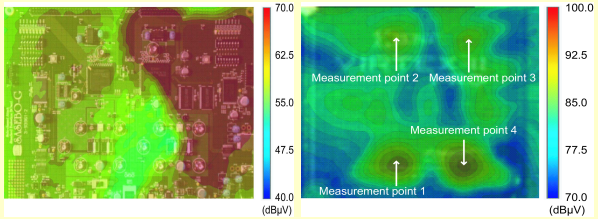
TARGETS : ASICs, FPGAs

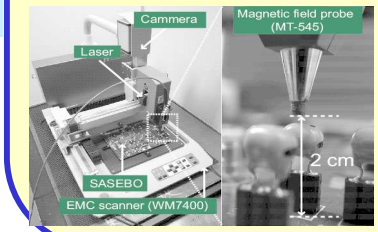
Real Circuit Analysis
- Analysis platform
- SCA, FA, SCARE, FIRE

Countermeasures Design
- DPL, masking, custom protection
- TRNG, PUF
- Secure Bus
- Protection at protocol level (resilience)

Model and Design Analysis
- Security automation
- Information theoretic metrics
- Formal proof

SPACES : EM Cartography





Publications:

« Practical Results of EM Cartography on a FPGA-based RSA Hardware Implementation » L Sauvage, S Guilley, j-L Danger, N Homma, Y Hayashi, EMC 2011.

« Identification of information leakage spots on a cryptographic device with an RSA processor » O Meynard, Y Hayashi, N Homma, S Guilley, JL Danger , EMC2011

SPACES : High-level Robustness Evaluation against SCA

Goal : To perform fast and accurate simulations to get a leakage level at High level modeling

Solution : To use a Bottom Up Gate level simulation approach

Principle : From Spice simulations create tabular models of current transitions and go up for Higher-Level primitives

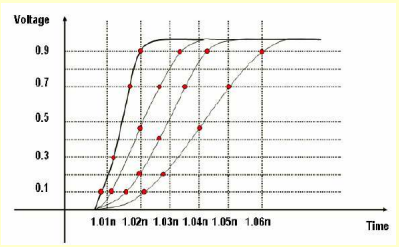
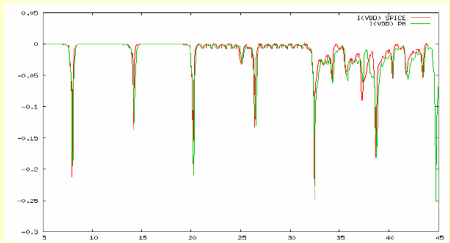


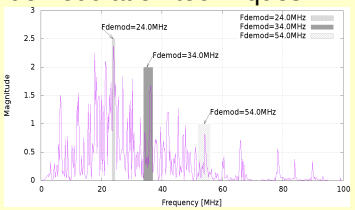
Table of current transitions

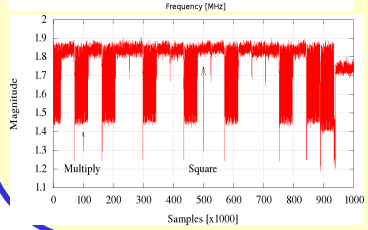


Power simulation of a 70K gates circuit (Cadence ECSM)

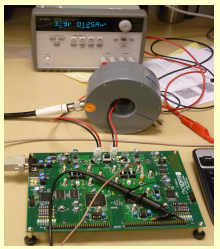
SPACES : Enhancement of EMA and FIA

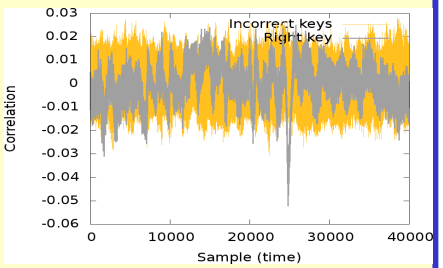
Enhancement of SEMA by demodulation techniques





EMI Fault Injection and use of sensible frequencies





Publications:

« Enhancement of Simple Electro-Magnetic Attacks by Pre-characterization in Frequency Domain and Demodulation Techniques » O Meynard, D Réal, F Flament, S Guilley, N Homma, J-L Danger, DATE 2011.

Workshop on Cryptographic Hardware and Embedded Systems 2011 (CHES 2011)
Nara, Japan, from September 28th to October 1st 2011