Mutualized Security Characterization Platform for Teaching, Research and Development

Anne-Lise RIBOTTA*
Bruno ROBISSON#
Assia TRIA#
Pascal MANET#

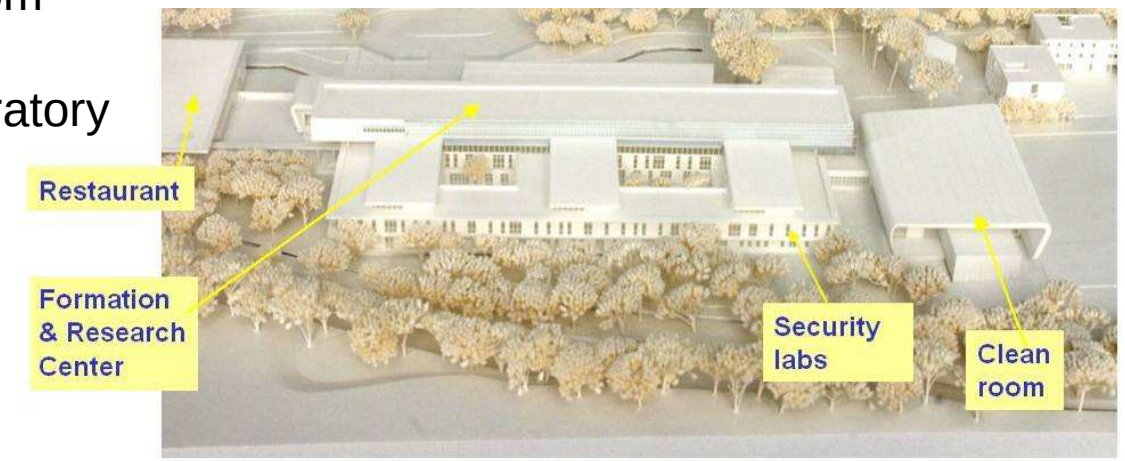
SESAM Laboratory (joint R&D team #CEA-LETI /*EMSE),
Centre Microélectronique de Provence
880 route de Mimet, 13541 Gardanne, France
Contacts: name@emse.fr
surname.name@cea.fr

Context

- In 2005, creation of an unique common research tool in France : « CIM PACA »
  - Three interconnected R&D platforms :
    - “Design platform”
    - “Characterization platform”
    - “MicroPackS platform”
  - Public/private partnership structure

- The MicroPackS platform works on flexible micropackaging and security characterization at ENSMSE-SGC in Gardanne.

  This platform is composed of :
  - 600m² of clean room
  - 90 m ² of security characterization laboratory



ENSMSE-SGC

Members

Founder members :

gemalto, ST, nbstech NBS TECHNOLOGIES, Smart Packaging Solutions, STid Identification Electronique, Ecole Nationale Supérieure des Mines SAINT-ETIENNE Centre Microélectronique de Provence Georges Charpak, leti, LIRMM Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier

Associated members :

Industrial:
ATMEL, ASK, Impika, Inside,
Academic:
L2MP/TECSEN (U1-U3),
GCOM2/LP3 (U2)

? **Your institution!** ?

Public fundings :

Région PACA, CONSEIL GENERAL, communauté du PAYS D'AIX, MINISTÈRE DE L'ÉCONOMIE DES FINANCES ET DE L'INDUSTRIE, ministère délégué à l'enseignement supérieur et à la recherche, EUROPA

Aims

The industrials are able to quickly characterize the security of their products and, if necessary, improve them before the certification process.

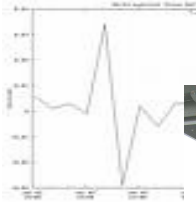
Small and medium enterprises have access to high end equipment at the lowest cost.

Academics are able to improve their knowledge on security and evaluate the efficiency of their counter-measures.

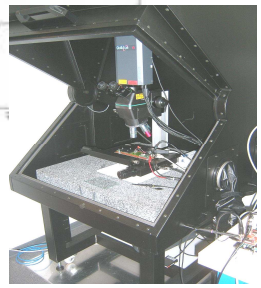
The lab is already used for training in security courses.

- Platform **is** :
  - A structure which gives access to R&D equipments
  - A place to develop innovative technology blocks
  - An organization to setup cooperative projects
- Platform **isn't** :
  - An academic lab
  - A service provider
  - An official evaluation lab (CESTI, ITSEF).

Opportunities

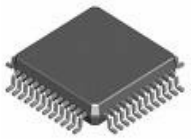


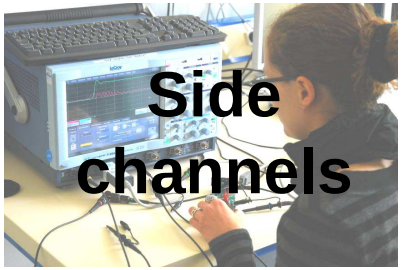
Faults



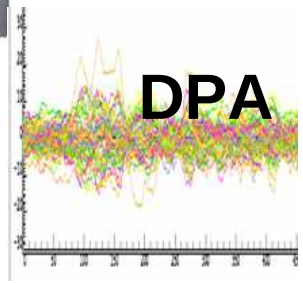
DFA

DUT





Side channels



DPA

Preparation *Acquisition* *Data extraction*

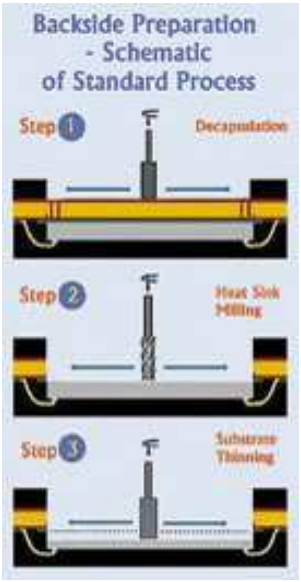
Estimation of the IC's security level

Ecole Nationale Supérieure des Mines SAINT-ETIENNE Centre Microélectronique de Provence Georges Charpak

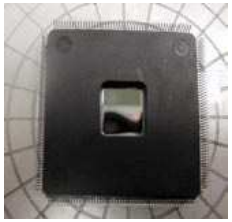
Micro-PackS

Preparation of components

– Thinning of packaged IC
  - Back side
  - Front side

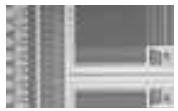


– Anti-reflective coating
  - Quality of picture during imaging
  - Impact of laser during attacks



Before

After



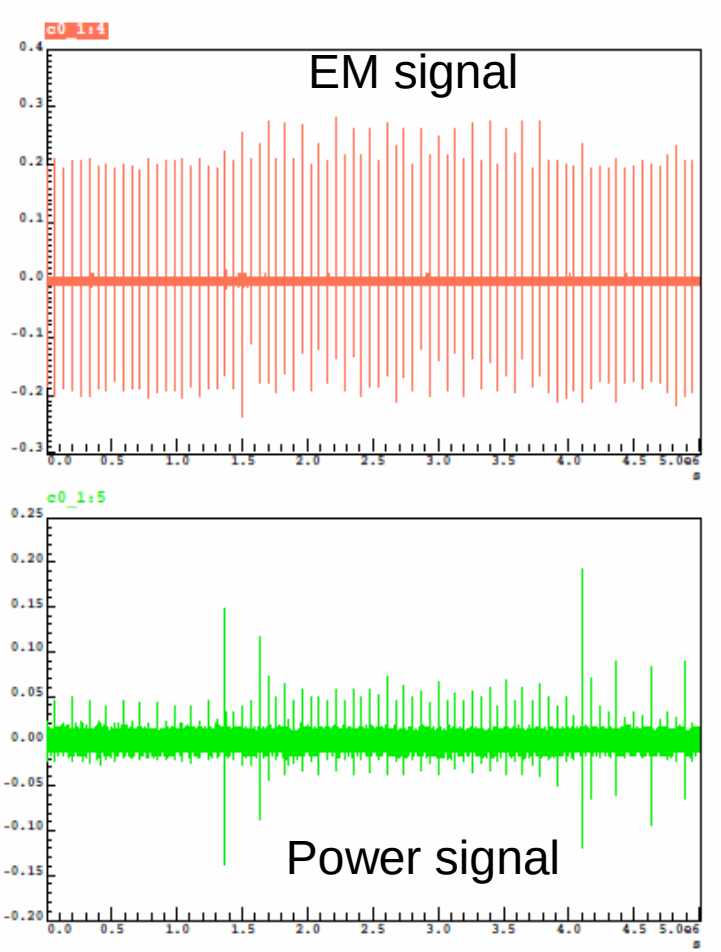
Cryptarchi08

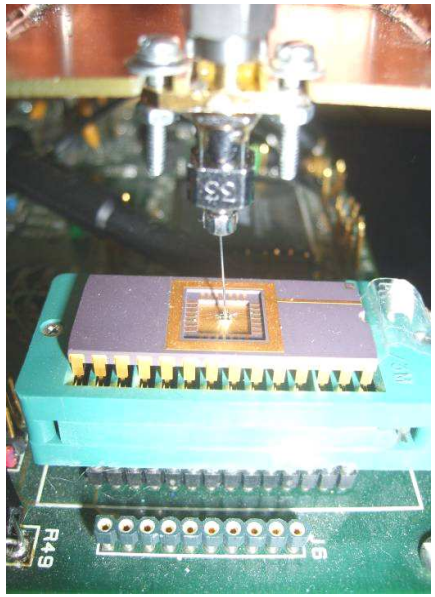
Ecole Nationale Supérieure des Mines SAINT-ETIENNE Centre Microélectronique de Provence Georges Charpak

Micro-PackS

Side channels

- Differential probes
- E and H probes
- High bandwidth oscilloscopes
- XY stage
- Camera
- ISO reader (optional)

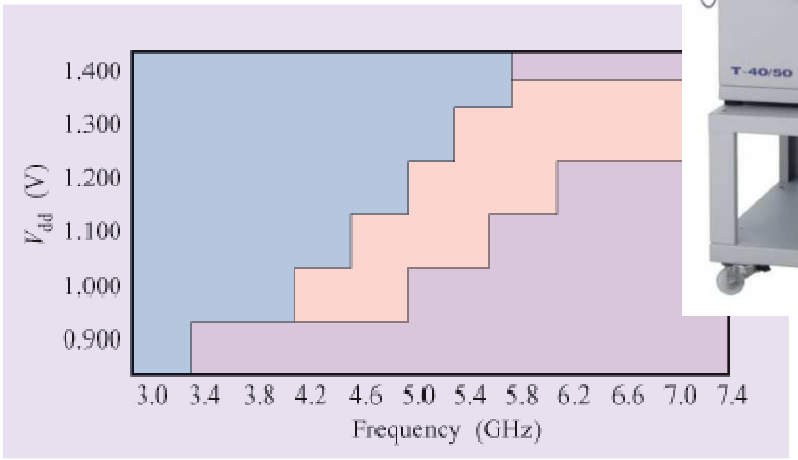




Electrical tests

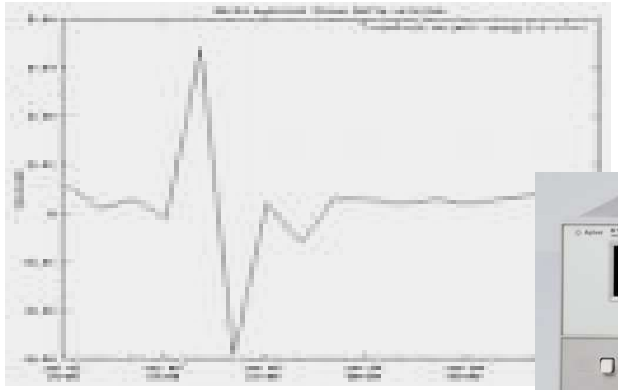
Parametrical test

- Voltage
- Temperature
- Clock



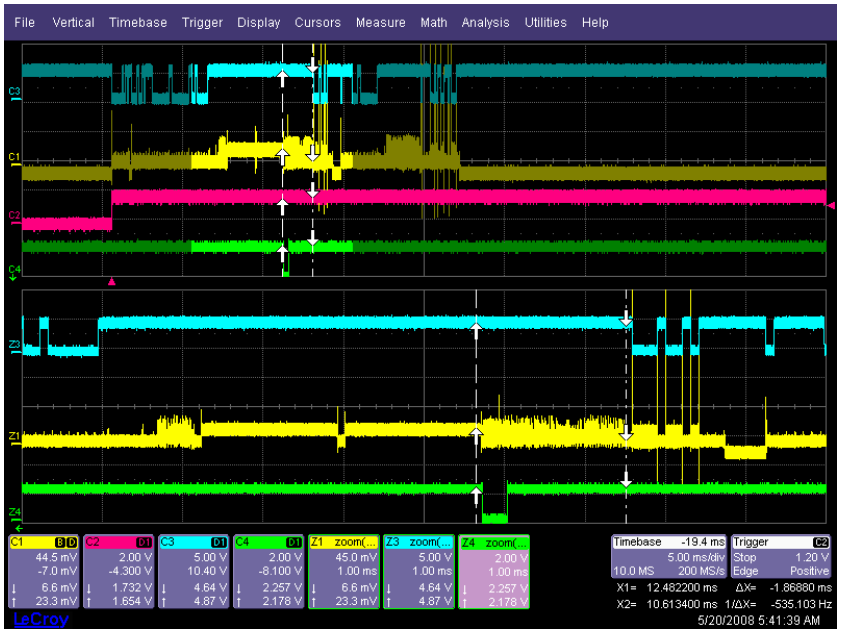
Glitches

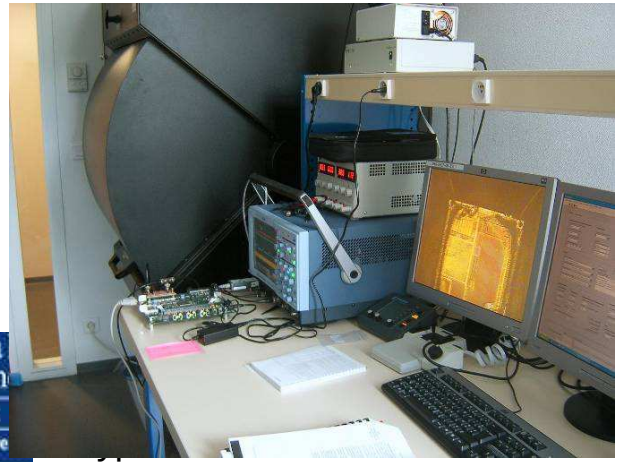
- Voltage
- Clock

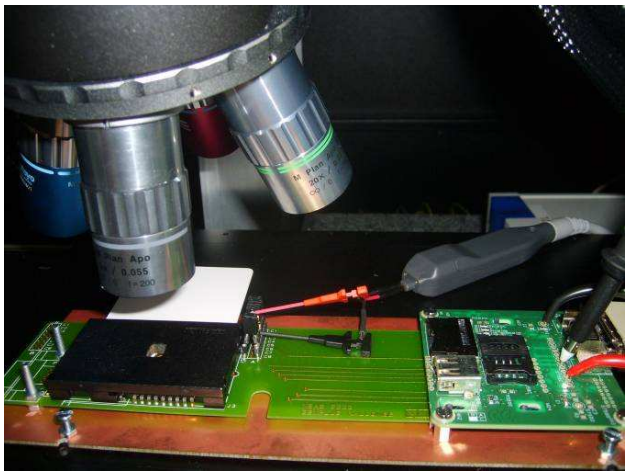


Laser

- Laser (IR, Green, UV)
- XY stage
- Camera
- Oscilloscope
- Synchronization board
- ISO Reader (optional)





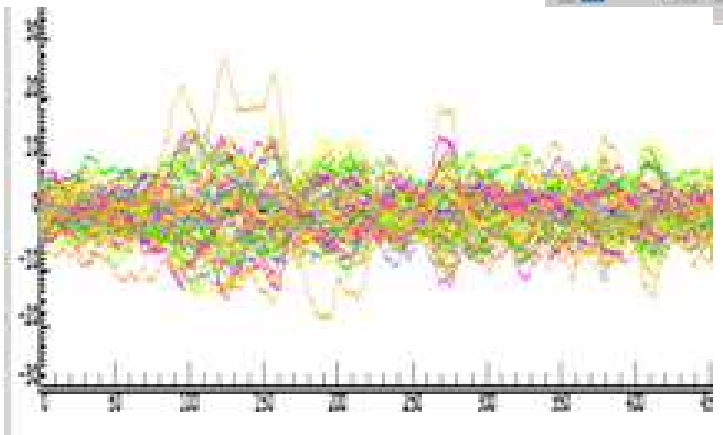


Ecole Nationa
Supérieure des Min
SAINT-ETIENNE
Centre Microélectronique de Prove
Georges Charpak

Micro-PackS

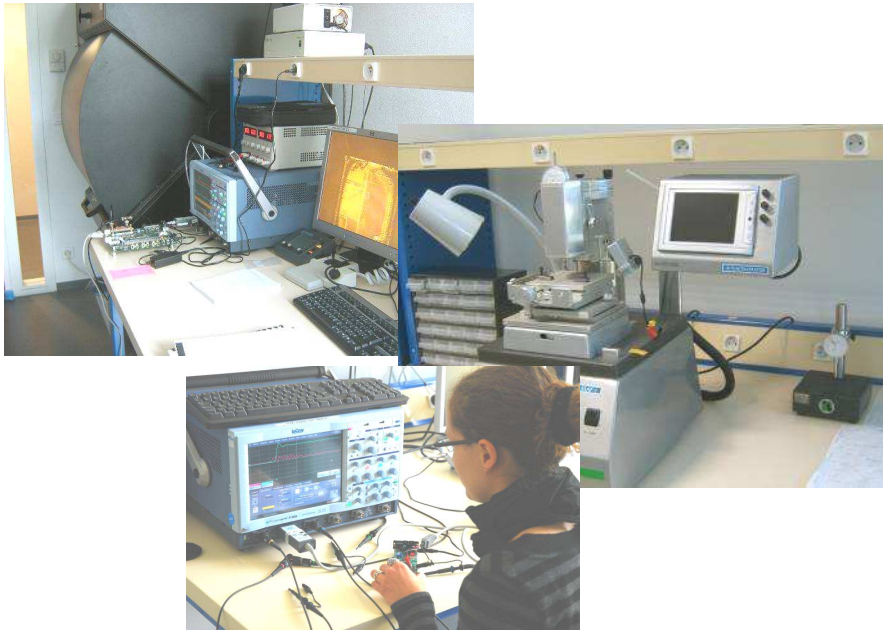
Servers and software tools

- Computational ressources
  - Sun server (8 processors, 16 GB RAM)
  - 1 TB HDD
  - Backup / recovery system
  - Available from each box
- Data extraction softwares
  - DPA
  - DFA
  - DBA



Around

Research projects
- BTRS
- Calisson
- SOS
- Sacose
- ...



Development
- Gemalto
- STM
- SPS
- PSI
-...

Education
- SISA master
-...

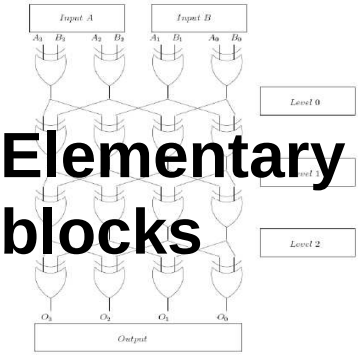
Research: tasks performed on the platform

BTRS

AES with fault and SCA counter-measures

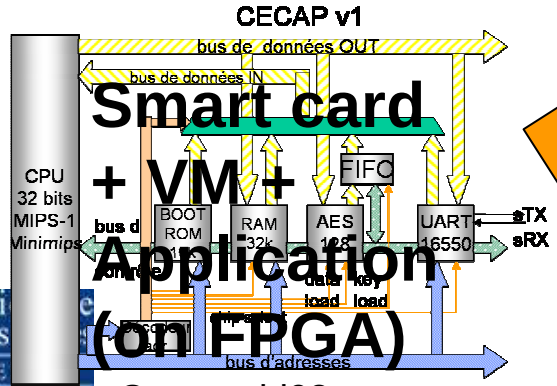
CALISSON

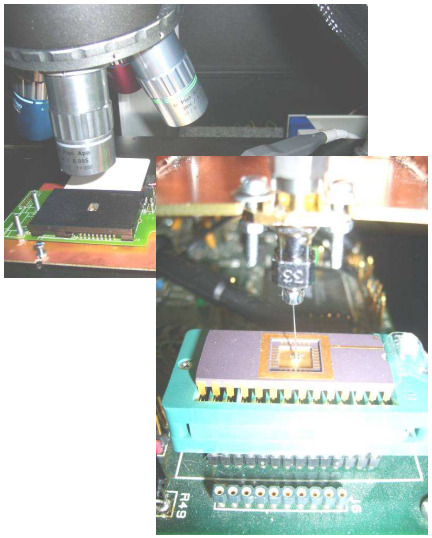
Elementary blocks



SOS

Smart card + VM + Application (on FPGA)





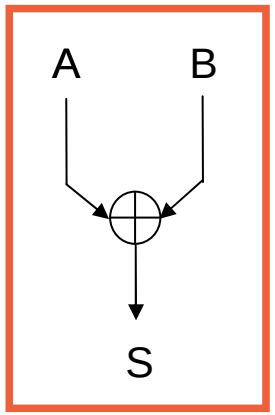
Security of ASIC crypto

Knowledge on syndroms

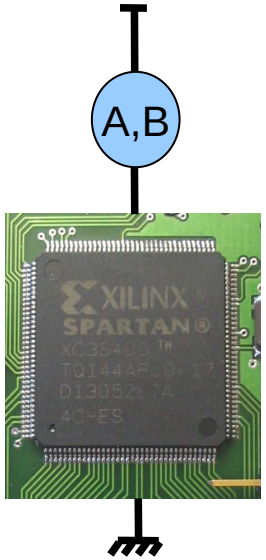
Security of FPGA based systems

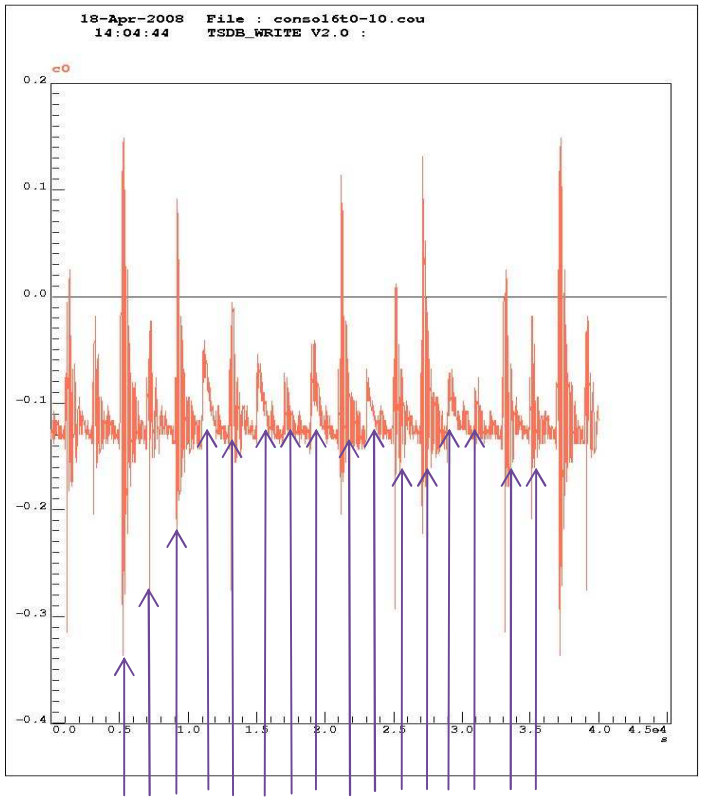
Education: lab “template on FPGA”

CELL



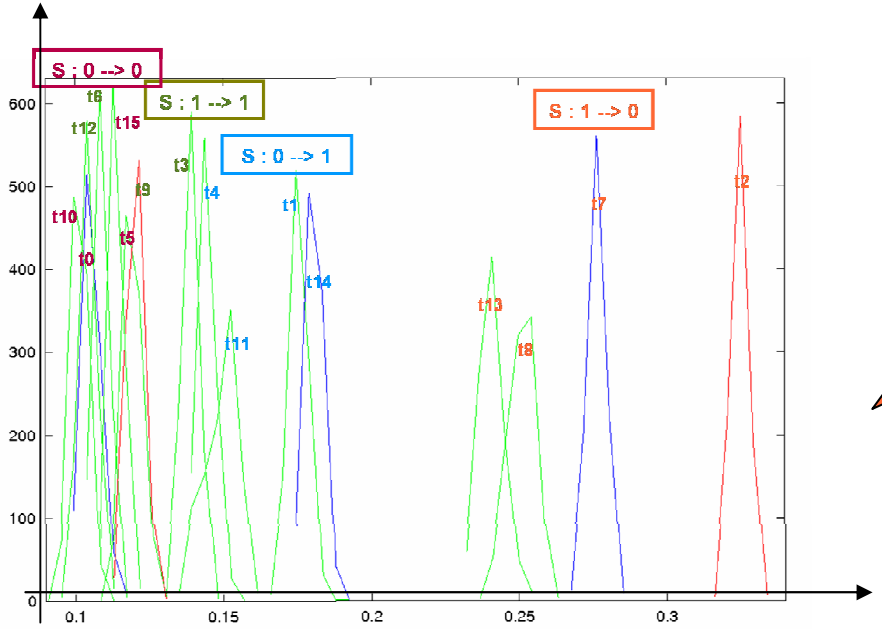
x 64





16 **transitions** = 16 **profiles**

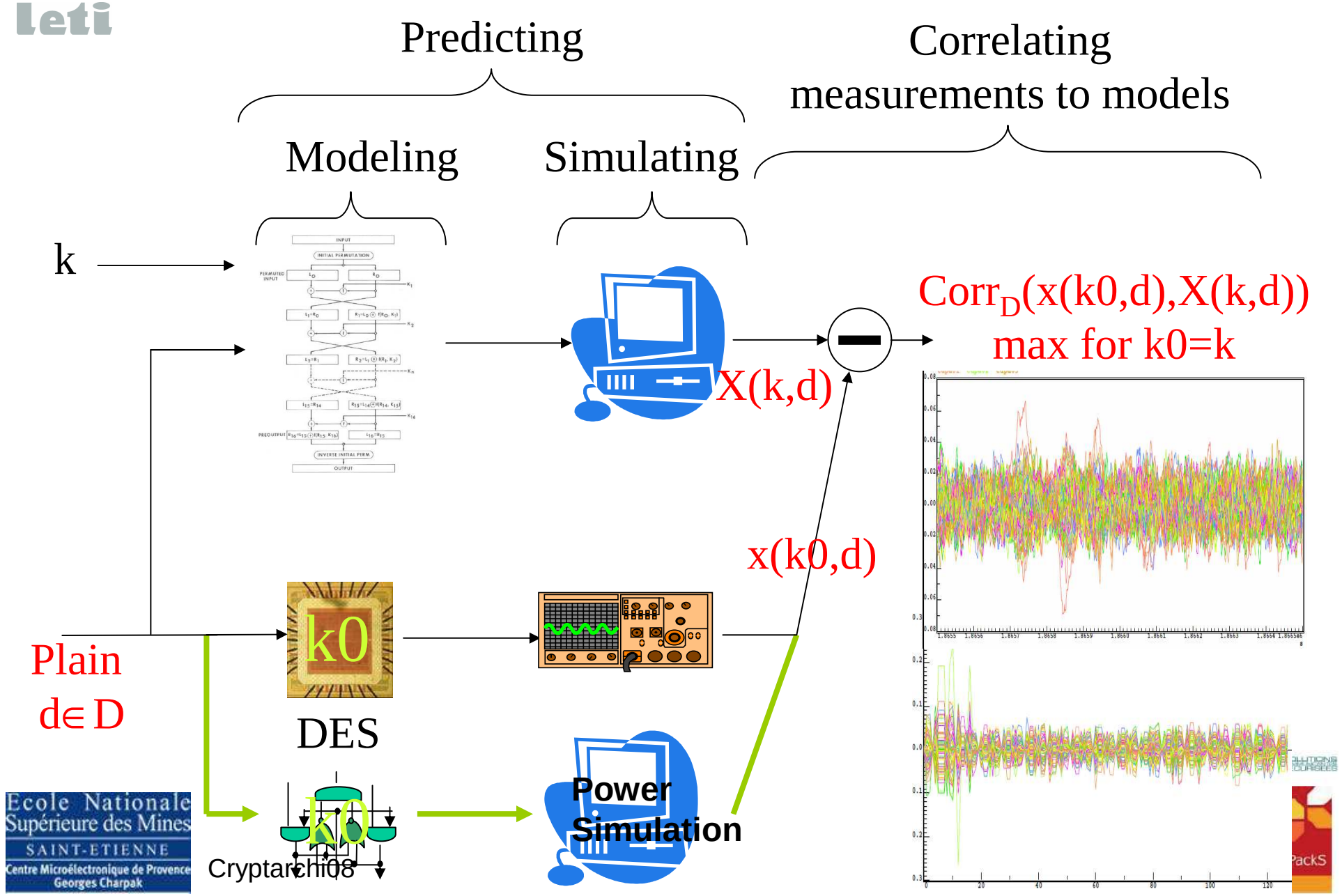
Number of realizations



Cryptarchi08

Maximum values of peaks

Education: lab “Differential Power Analysis”



Enhancements

- Shortcoming equipments
  - Addition of IR camera to laser bench
  - More EM probes
  - Contactless bench

- Future equipments
  - Advanced Laser bench
  - More preparation tools

Thanks!