LIESSE
Laser-Induced fault Effects in Security-dedicated circuitS

http://www.anr-liesse.fr/index.php/fr/
1 – CONTEXT

- Security is everywhere: Banking, E-commerce, Identification, ...
- Main issues
  - Confidentiality (data & messages): AES, DES/3DES, RC5
  - Integrity (data & messages): MD5, SHA-1, SHA-2
  - Authentication (users & hosts): RSA, ECC
- Hardware implementations
  - Smarcards, Electronic signature, Access control for restricted areas or systems, Electronic purse, set-top box ..
- Algorithms proven to be resistant (against brute-force or cryptanalysis attacks). But ....
- Hardware subject to attacks
  - Intrusive attacks (e.g. reverse engineering, probing, ...)
  - Side-channels attacks (power, EM or light emission, ...)
  - Fault attacks
1 – CONTEXT

- Differential Fault Attacks (DFA)
  - Principle: compare results of normal operation vs "faulted" ones => deduce secret information
  - Safe errors, direct hacking, protection bypass ...

- Useful faults: right time & right localisation

- Fault injection
  - Glitch on supply voltage or external clock
  - Electromagnetic wave, X-ray, ion beams
  - Temperature variation
  - Laser illumination
Laser offers fine control on:

- location,
- timing (choice of the injection cycle),
- focalization (i.e. number of faulted bits)

Semi-invasive attack: chemical/mechanical package opening


G. Piret, J.-J. Quisquater: A Differential Fault Attack Technique Against SPN Structures, with Application to the AES, CHES 2003, LNCS 2779, Springer-Verlag
1 – CONTEXT

Energy of the laser

> Energy of the band gap of the silicon

Induced photocurrent

V1 = Vdd

V2 = gnd

P-substrate

SCR

h+/e- separation

P+
Iph = f(Power_{laser}, Area_{pn}, Distance_{pn}, Time_{laser}, \ldots)

**Transient current**

=> **Transient voltage pulse**

=> **Fault/Error**

SET on combinational
SEU on memory elements
2 – LIESSE PROJECT

Main Objectives

1/ Provide to designers early evaluation tools
   • CMOS technologies sensitivity vs laser
   • Fault models
     • C-MOS technology
     • Laser characteristics
   • Experiments on prototypes
   • Specific CAD tools

2/ Robustness & Counter-measures evaluation
   • Simulation
   • Emulation

3/ Counter-measures proposals
Main Objectives

- Laser characteristics, measures
- Laser fault/error models
  - Physical
  - Electrical
  - Logical
  - Behavioral

Design (RTL)

Early robustness evaluation

Add. Counter-measures, lower-level design steps

Final design-time robustness evaluation

Qualification
3 – Test Vehicles & Technologies

- 90nm, 130 nm circuit available
- New technologies: 28nm Bulk, 28nm FD-SOI

3 specific designs (circuits + boards)

- Elementary elements: PN junctions, Transistors, Diodes, etc. (fabricated)
  28 nm Bulk & SOI
- AES 28nm bulk (fabricated)
- AES 28nm SOI (under development)
3- Fault Models: Physical level

- Laser modelling:
  - Depending with laser energy, spot size, ...
  - Requirement: 3D charge deposition, dynamics, energy → carrier density

\[
I(r, z) = I_o \cdot e^{\frac{-2.r^2}{\omega(z)^2}} \cdot e^{-\alpha.z}
\]

\[
\omega(z) = \omega_o^2 \left(1 + \left(\frac{\lambda.(z - z_0)}{\pi.n.\omega_o^2}\right)^2\right)
\]

Laser model:

\[n \text{ (e-h/cm3)} \rightarrow I(t)\]
3- Fault Models: Measures vs Models

Laser-induced transient current in an NMOS

Laser impulsion : 20µs, 1.25W, $V_{\text{drain}}$ = 1.2V, $V_{\text{gate}}$ = $V_{\text{source}}$ = $V_{\text{bulk}}$ = 0V

Measures :

Simulation :

Currently : 28nm FD-SOI
3- **Electrical Modeling**

<table>
<thead>
<tr>
<th></th>
<th>FDSOI</th>
<th>Bulk</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NMOS</strong></td>
<td><img src="image1" alt="NMOS FDSOI" /></td>
<td><img src="image2" alt="NMOS Bulk" /></td>
</tr>
<tr>
<td><strong>Structure</strong></td>
<td><img src="image3" alt="NMOS Structure" /></td>
<td><img src="image4" alt="NMOS Structure" /></td>
</tr>
<tr>
<td><strong>Modèle</strong></td>
<td><img src="image5" alt="NMOS Modèle" /></td>
<td><img src="image6" alt="NMOS Modèle" /></td>
</tr>
<tr>
<td><strong>PMOS</strong></td>
<td><img src="image7" alt="PMOS FDSOI" /></td>
<td><img src="image8" alt="PMOS Bulk" /></td>
</tr>
<tr>
<td><strong>Structure</strong></td>
<td><img src="image9" alt="PMOS Structure" /></td>
<td><img src="image10" alt="PMOS Structure" /></td>
</tr>
<tr>
<td><strong>Modèle</strong></td>
<td><img src="image11" alt="PMOS Modèle" /></td>
<td><img src="image12" alt="PMOS Modèle" /></td>
</tr>
</tbody>
</table>
3- Fault Models: from Physical to Electrical level

- Layout of standard cells (.gds)
- I(t) database of standard cells
- Electrical fault model
4- CAD TOOLS

- **Simulation:**
  - Laser parameters
  - Spot location vs Circuit layout
  - Accurate fault models

- **Emulation**
  - High level resistance evaluation
  - Realistic fault model
4- SIMULATION

Circuit Layout + Laser spot

To locate the affected pn-junction

To look up $I(t)$ from MUSCA generated database

Logic-level fault simulation

HSPICE simulation

tLIFTING : Multi-level simulator
4 - Process of Multi-level Fault Simulation

Legend:
- 0-delay Logic-level
- Delay-annotated Logic-level
- Analog-level

100% Accurate (vs Spice)
500 x Faster
Use of functional relations in RTL description taking into account laser shot locality in order to inject multiple errors taking into account the laser locality.
5 - COUNTERMEASURES

- Cell-Based Laser Sensor

Cost: 4.2% area overhead
Fault detection: 99%
5- **COUNTERMEASURES**

- **Technological**:  
  - FDSOI more robust than Bulk
- **Sensors**:  
  - BBICS: Built-in potential/current sensors  
  - Deep Trench Isolation (DTI)  
  - Light sensors
- **Layout modification (AES)**
- **Logic cone partitionning**
- **Low-cost error correction with hybrid redundancy**
- **Dynamic data relocation**
MAIN RESULTS

- Electrical modeling of laser on deep-micron CMOS 28nm Bulk and FDSOI.
- Experimental proof of less sensitivity of FDSOI technologies vs Bulk ones.
- An FPGA-based emulation fault injection platform (RTL early sensitivity evaluation).
- Calibration of physical models for exhaustive study on elementary logic cells, alternative to TCAD.
- Open-source software for simulation and emulation.
- Countermeasures
CONCLUSIONS

- Liesse is a research project to build really efficient evaluation tools and solutions
  - Geared towards designers
  - A set of silicon/laser interaction models to fit with design flow
  - CAD tools
    - Early design evaluation
  - Countermeasures


"Layout-Aware Laser Fault Injection Simulation and Modeling: from physical level to gate level", L. Feng, M.L. Flottes, B. Rouzeyre, G. Hubert, 9th International Conference on Design & Technology of Integrated Systems in Nanoscale Era” (DTIS), 2014


Increasing the security level of analog IPs by using a dedicated vulnerability analysis methodology”, N. Beringuier-Boher, D. Hely, V. Beroule, J. Damiens, P. Candelier, 14th International Symposium on Quality Electronic Design (ISQED 2013)