

Body Biasing Injection Attacks in Practice

Noemie Beringuier-Boher¹, Marc Lacruche¹, David El-Baze¹, Jean-Max Dutertre¹, Jean-Baptiste Rigaud¹, Philippe Maurine²

¹: SAS, Mines Saint-Etienne, Gardanne France

²: LIRMM, Montpellier France

- Body Biasing Injection Attacks
- Evaluation Bench
- Physical Effects
- Conclusion and Perspectives

Body Biasing Injection Attacks

- 2 main kinds of hardware attacks:
 - Side Channel Analysis (SCA)
 - Fault Injection Attacks
- Lot of fault injection methods (Laser, Supply Voltage, etc...) widely studied and with a lot of countermeasures
- **Can we find new fault injection method?**

Body Biasing Injection Attacks

- Presented by K.Tobich et al. in 2012
- Apply a high magnitude transient voltage pulse
- On the circuit substrate (request backside access and package opening)
- Positive or negative pulses

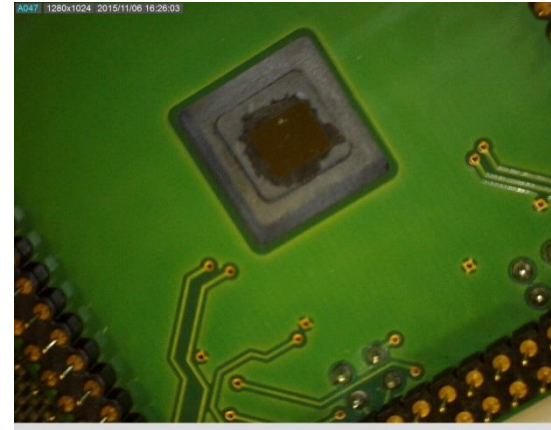


Fig. 1 : A backside opened micro-controller

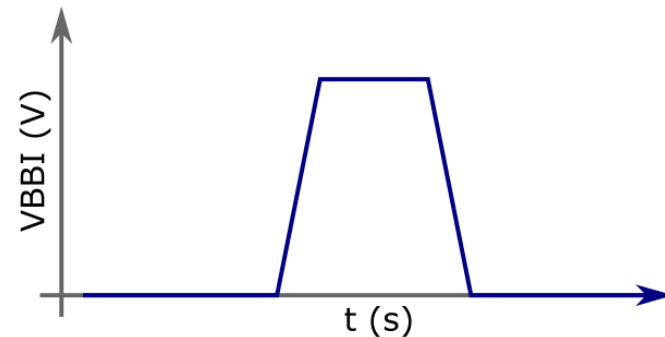


Fig. 2 : A BBI voltage pulse

- For basic BBI attacks:
 - Backside opened circuit
 - Micro-probe tip
 - Transient voltage pulse generator
 - Oscilloscope
 - Computer
- For sensitivity maps:
 - XYZ stage
 - Weighing scale

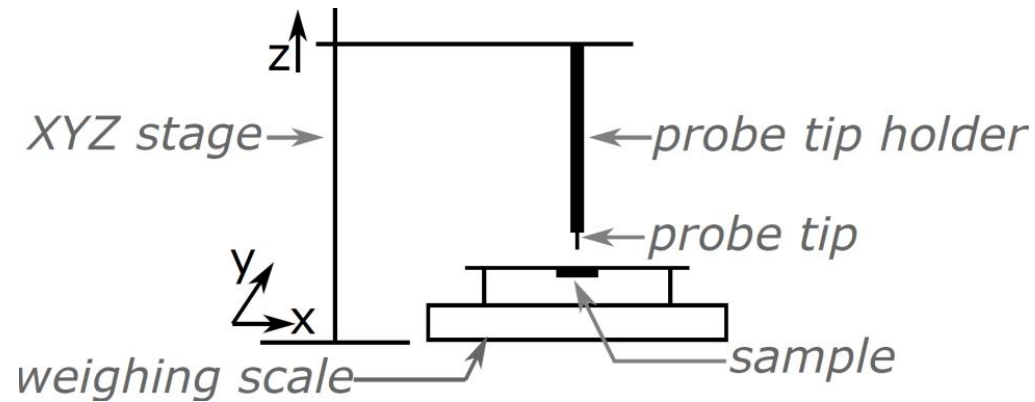


Fig. 3 : Schematic view of the evaluation bench

- Various attack parameters:
 - Voltage pulse shape
 - Micro-probe tip diameter and contact resistivity
 - Substrate thickness and resistivity
- Main difficulties:
 - Find the appropriate pulse shape
 - Replace the probe properly during sensitivity mappings



Fig. 4 : Damaged circuit (hole in silicon)



Fig. 5 : Correct and damaged probe tip ends

- A first order model build by K. Tobich et al.
- Considers couplings between the external environment, the circuit substrate and the internal power supply nodes
- Does not takes into account internal CMOS logic couplings

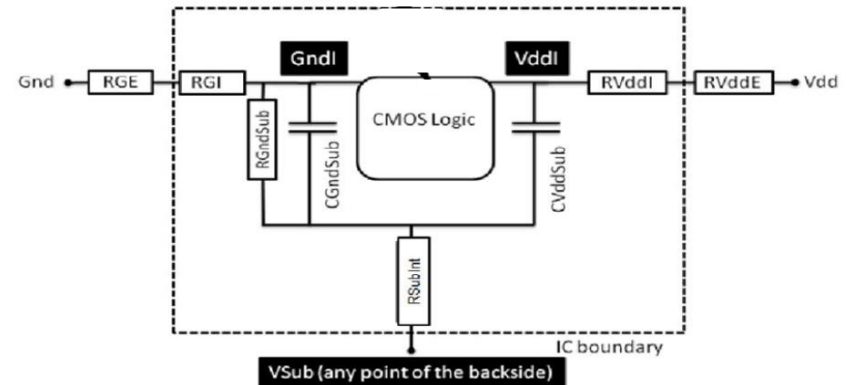


Fig. 6 : 1st order model of an IC power and ground networks

- Physical model based on RC couplings between VddI and GndI
- Plus a diode between PMOS and Psub
- Diode activation only for positive pulses (FBBI)

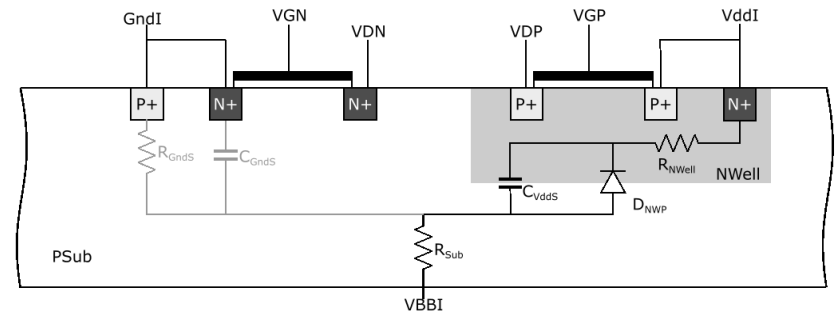


Fig. 7 : BBI effects on CMOS logic (cross sectional view)

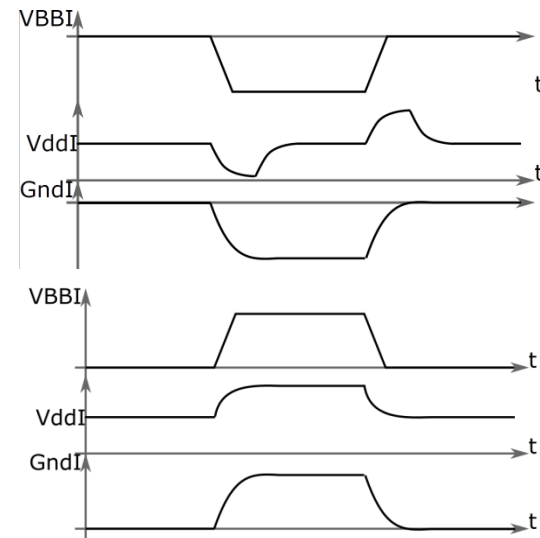


Fig. 8 : RBBI and FBBI effects on VddI and GndI nodes

Preliminary Results

9

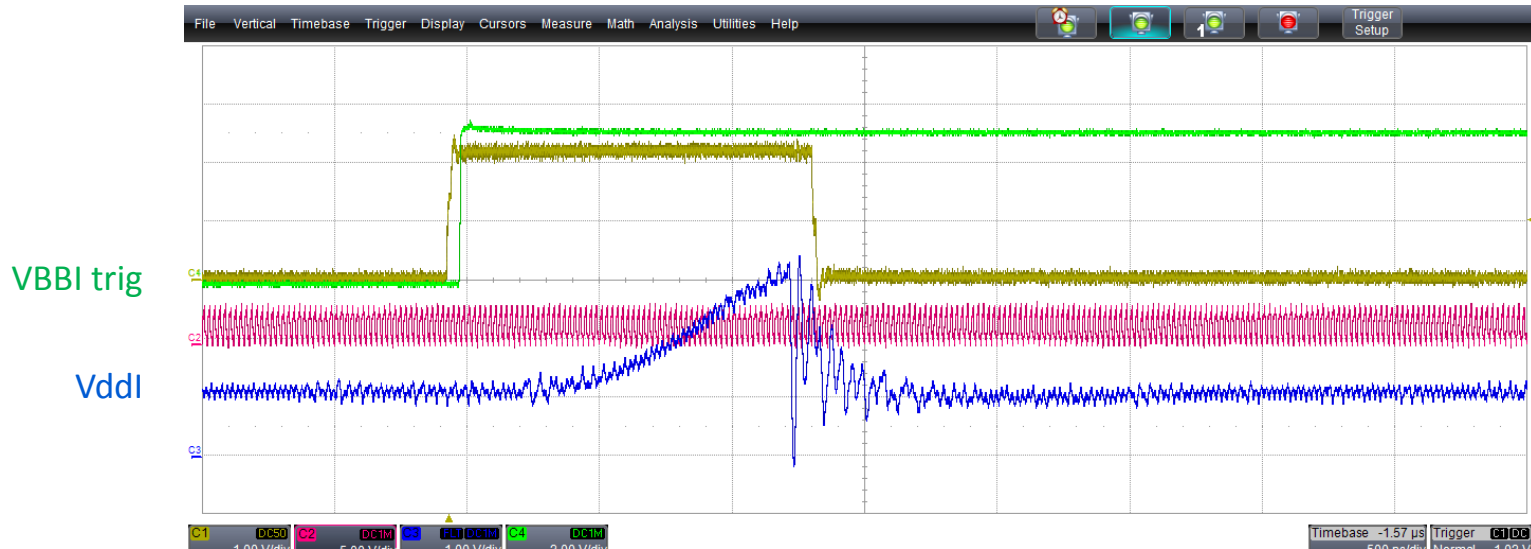


Fig. 9 : Validation of the physical model

- Response shape ok
- A BBI pulse of +60V during $8\mu\text{s}$ leads to a +2.3V, $1\mu\text{s}$ pulse on VddI (here on a CMOS 90nm microcontroller)
- Depends on the RC coupling values

Preliminary Results

10

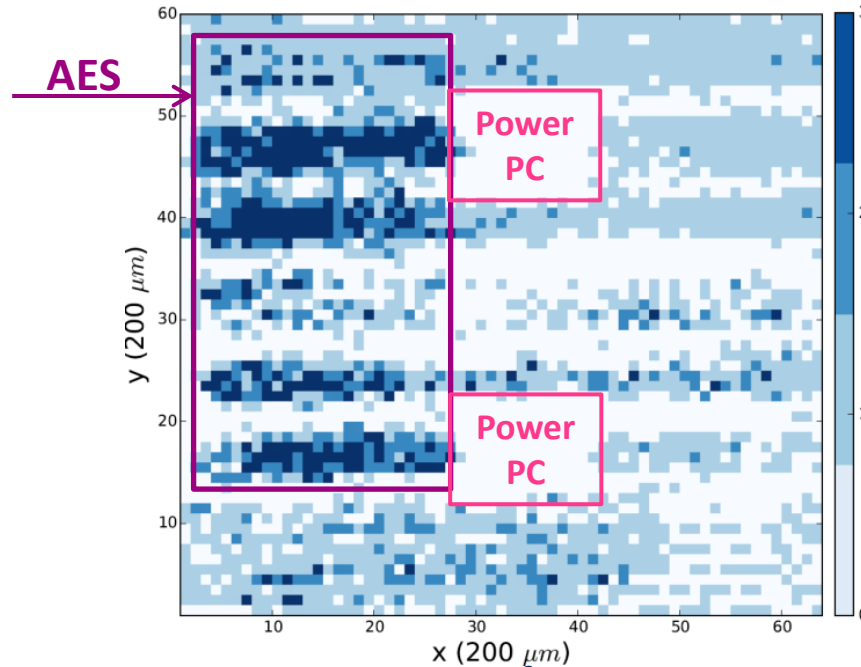


Fig. 10 : Sensitivity map of a CMOS 90nm FPGA

- 60*64 points map (X and Y spaces =200μm)
- -160V, 200ns BBI pulses
- Number of faulty cipher text for each position and for 3 AES computations

Conclusion and Perspectives

- An accurate and low cost evaluation bench has been presented
- The physical effects of BBI attacks on CMOS logic has been analyzed
- The sensitivity map provided shows the local effect of BBI attacks
- Further work will include:
 - Analysis of the fault propagation mechanism and fault model investigation (e.g. timing violations, etc.)
 - Attack parameters influence