Electromagnetic Transient Faults Injection

• François Poucheret
• Philippe Maurine
• Amine Dehbaoui
• Bruno Robisson
• Assia Tria
• Jean-Max Dutertre
• François Poucheret
• Philippe Maurine
Embedded Secure System Evolution

Nowadays Secure Devices

Next Secure Devices?

- $10 \times 10^2$ GHz
- $10$ MHz
- $10$ mW
- $100$ W
Is it possible to inject fault in such systems?

- ~100 k gates, 
  ~ 30 MHz, 
  ~ 5 mm² 
  ~ 90 nm / 4 metal layers

- ~1 M gates, 
  ~ 1 GHz, 
  ~ 25 mm² 
  ~ 45 nm / 7-10 metal layers

Easy access to frontside and backside!

Access to backside is difficult! BGA packages !!!
Motivations for EMP Injection

• Does not require depackaging the target
• Does target the upper metal Layer (Vdd, Gnd, Clk)
• May bypass some countermeasures (light sensors, global power filtering …)

Seems adequate to inject fault in Secure SoC designed with advanced technologies!
Agenda

- What is a EMP platforms ? Is it low Cost ?
- Does it always works ?
- What is the effects of an EMP platform on IC?
- What is the resolution of an EMP ?
EMP platforms

A control PC

Pulse Generator

A magnetic Probe

Low Amplitude Pulses (CEA-EMSE)

- Amplitude: 1 V - 100 V
- Pulse width: 9 ns – 1 ms
- Rising/falling times: 5 ns
- Very low jitter: < 45 ps

- Rohde & Schwartz magnetic antenna (500µm diameter)

High Amplitude Pulses (LIRMM)

- Amplitude: 100 V – 1.2 KV
- Not Available on the market
- Must be home made

According to both the Amplitude and Repetition Rate
EMP Injection: Observation

Low Amplitude Pulses:
- \( \Delta V = 50\text{V} \)
- Width = 20 ns
- 150 mV Voltage Drop (Vdd noise)

High Amplitude Pulses:
- \( \Delta V = 900\text{V} \)
- Width = 250 ns
- 300 mV Voltage Drop

Vdd (mV)

<table>
<thead>
<tr>
<th>100</th>
<th>200</th>
<th>300</th>
</tr>
</thead>
<tbody>
<tr>
<td>150</td>
<td></td>
<td></td>
</tr>
<tr>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-150</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

50 ns

150 mV

300mV Voltage Drop

200 mA

100 ns

Ignd
EMP Injection: Design considerations

\[ \tau \approx 2 \cdot \frac{L^2}{\mu \cdot \left( V_{DD} - V_t \right)^2} \]

\[ \text{Delay} \approx a \cdot \tau \cdot \frac{C_L}{C_{IN}} \]

\[ \text{Timing}_{-} \text{Slack} = T_{CK} - \delta - T_{\text{SETUP}} - [\text{CK}_2Q + \text{Q}_2D] \]

IC are designed to tolerate:
\[ V_{\text{drops}} < 0.1 \cdot V_{dd} \]
EMP Injection: Effect

65 nm

Designs are designed to operate correctly with such timings!

Clock related Timing constraint

EM Pulse

Vdd

Minimum Voltage

Nominal Voltage
Validations & Experimental Results

Experiments

1. Hardware AES 50 MHz
   - Xilinx Spartan 3
   - Core supply: 1.2 Volts
   - Clock speed: 50 MHz
   - Tslack = 10 ns

2. Hardware AES 100 MHz
   - Xilinx Spartan 3
   - Core supply: 1.2 Volts
   - Clock speed: 100 MHz
   - Tslack = 2 ns

3. Hardware AES 100 MHz + CM
   - Xilinx Spartan 3
   - Core supply: 1.2 Volts
   - Clock speed: 100 MHz
   - Tslack = 2 ns
   - Embedded countermeasure
   - Detection of timing violations
Validation & Experimental Results

Hardware AES
50 MHz

- Xilinx Spartan 3
- Core supply : 1.2 Volts
- Clock speed : 50 MHz

Tslack = 10 ns

2500 injections:
98% of faulted texts
@ 600 V

350 Mono-bit faults

Multi-bits faults
Less than 16 bits faulted

Multibits faults
More than 16 bits faulted

# of faulted bits
EMP Injection Cartography

- At each position, an EMP is injected during the last round of the AES.
- The corresponding faulted ciphertext (if any) is retrieved.
- This process is done for **1,000 encryptions** of the same plaintext.
- This process is done for **30x30 different locations** of the injection probe on top of the FPGA.

Fault occurrence versus EMP amplitude

- Localized effect of the EMP.
- Good correlation between the Floorplan and the cartography.

T_{\text{slack}} = 2 \text{ ns}
Localized Effect of the Voltage Drops

Faults cartography

Faulted bytes

Mono-bit faults
Multi-bit faults
Voltage Drops Detection

- FPGA Spartan 3 XC3S1000 FT256
- Techno 130nm
- Operating voltage: 1.2 volts
- Operating frequency: 100 MHz
- Hardware AES implementation
- countermeasure (detection of timing violations)
Voltage Drops Detection

- At each position, an **EMP** is injected during the last round of the **AES**
- The corresponding faulted ciphertext (if any) is retrieved
- The value of the alarm flag is stored
- This process is done for **1,000 encryptions** of the same plaintext
- This process is done for **30x30 different locations** of the injection probe on top of the FPGA

![Alarms cartography](image1)
![Faults cartography](image2)

- Localized effect of the **EMP**
- The EMP is detected only in some positions
- Possibility to induce faults without triggering the alarm
Spatial Resolution?

CST simulations
H field
1 turns / Ø 100 µm
200 µm below the probe

Resolution of EMP Injection depends of the IC!

D=0.7 mm

50 % of Energy
Conclusion & Further works

- Ability to inject **single-bit** and **multi-bits** faults into AES calculations

- Induced faults are timing faults due to voltage drops

- EMP amplitude depends on Timing slack (IC frequency and technology)

- **Localized effect**: the coupling depends of the IC Layout

- May **bypass** power supply low-pass **filtering**

- May fault any paths (even non critical paths)