Laser Fault Injection at the CMOS 28 nm Technology Node: an Analysis of the Fault Model


Amsterdam, The Netherlands — Thursday, September 13, 2018
A brief history of laser fault injection

1965  Habing introduced laser emulation of SEE
      Emulation of radiation induced Single Event Effects

1997  Boneh et al. introduced fault attacks
      Hardware attack of crypto./secure devices

2002  Skorobogatov et al. introduced laser fault inject.
      Secure devices: CMOS 350 nm
      One single transistor under a laser beam (1 µm)

2018  Continuous scale down of CMOS technology
      Secure devices: CMOS 40 nm
      SoC: CMOS 14 nm
      Several logic gates under a laser beam (1 µm)
LFI accuracy vs. CMOS scale down

<table>
<thead>
<tr>
<th>Technology</th>
<th>MOS transistor</th>
<th>SRAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.35 µm</td>
<td>![Image]</td>
<td>![Image]</td>
</tr>
<tr>
<td>130 nm</td>
<td>![Image]</td>
<td>![Image]</td>
</tr>
<tr>
<td>90 nm</td>
<td>![Image]</td>
<td>![Image]</td>
</tr>
<tr>
<td>65 nm</td>
<td>![Image]</td>
<td>![Image]</td>
</tr>
<tr>
<td>28 nm</td>
<td>![Image]</td>
<td>![Image]</td>
</tr>
</tbody>
</table>
### LFI accuracy vs. CMOS scale down

<table>
<thead>
<tr>
<th>Technology</th>
<th>MOS transistor</th>
<th>SRAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.35 µm</td>
<td><img src="image" alt="MOS transistor" /></td>
<td><img src="image" alt="SRAM" /></td>
</tr>
<tr>
<td>130 nm</td>
<td><img src="image" alt="MOS transistor" /></td>
<td><img src="image" alt="SRAM" /></td>
</tr>
<tr>
<td>90 nm</td>
<td><img src="image" alt="MOS transistor" /></td>
<td><img src="image" alt="SRAM" /></td>
</tr>
<tr>
<td>65 nm</td>
<td><img src="image" alt="MOS transistor" /></td>
<td><img src="image" alt="SRAM" /></td>
</tr>
<tr>
<td>28 nm</td>
<td><img src="image" alt="MOS transistor" /></td>
<td><img src="image" alt="SRAM" /></td>
</tr>
</tbody>
</table>

Simultaneous flip of several SRAMs?
Importance of the fault model

LFI considered as an accurate fault injection technique:

• physical location (gates under/close to the laser spot),
• injection time (regarding the course of an algorithm),
• nb. of faulted bits/bytes,
• additional information leakage (data dependence).

Makes it possible to meet the (sometimes strong) requirements of FA and DFA schemes.

Does CMOS technology scale down reduce the accuracy of the laser fault injection fault model?
Fault model of LFI at the CMOS 28 nm tech. node

On an experimental basis (custom test chip)

- Single-bit/single-byte fault model
- Data dependence: bit-flip vs bit-set/reset fault model
- Static LFI on D flip-flops
- Dynamic LFI on an AES encryption unit
I. Introduction

II. Theory of laser fault injection
   Physics and basics of laser fault injection
   Fault models of LFI

III. Static LFI experimental results
   Setup, results, analysis

IV. Dynamic LFI experimental results
   Setup, results, analysis

V. Conclusion
I. Introduction

II. Theory of laser fault injection
   Physics and basics of laser fault injection
   Fault models of LFI

III. Static LFI experimental results
   Setup, results, analysis

IV. Dynamic LFI experimental results
   Setup, results, analysis

V. Conclusion
II. Theory of laser fault injection

- Physics of laser fault injection
  - Photoelectric effect: from a laser pulse to transient current generation (in reverse biased PN junction)
II. Theory of laser fault injection

- Fault injection mechanism (the inverter case)
  from a transient current to a voltage transient (a.k.a. SET, single event transient)
II. Theory of laser fault injection

- **Fault injection mechanism** (the inverter case)
  from a transient current to a **voltage transient** (a.k.a. SET, single event transient)
II. Theory of laser fault injection

- Fault injection mechanism (the inverter case)
  from a transient current to a voltage transient (a.k.a. SET, single event transient)
II. Theory of laser fault injection

- Fault injection mechanism (the inverter case)
  from a transient current to a voltage transient (a.k.a. SET, single event transient)

Laser sensitive areas: OFF transistors’ drains (reversed biased PN junctions)
Fault injection mechanism
from a voltage transient to an actual fault

Two mechanisms depending on the voltage transient location:
1. logic,
2. memory element (D flip-flop, SRAM)
II. Theory of laser fault injection

- Fault injection mechanism – target: combinatorial logic from voltage transient to fault
II. Theory of laser fault injection

- Fault injection mechanism – target: combinatorial logic from voltage transient to fault
The fault injection process depends both on:

- the injection time,
- the voltage transient duration.
II. Theory of laser fault injection

- Fault injection mechanism – target: D latch from voltage transient to fault (SEU: single event upset)

SEU sensitive for $Q = 0$
II. Theory of laser fault injection

- Fault injection mechanism – target: D latch from voltage transient to fault (SEU: single event upset)

SEU sensitive for $Q = 0$
II. Theory of laser fault injection

- Fault injection mechanism – target: D latch from voltage transient to fault (SEU: single event upset)

- SEU sensitive for Q = 0
II. Theory of laser fault injection

- Fault injection mechanism – target: D latch from voltage transient to fault \((SEU: \text{single event upset})\)

Note the data dependence of the laser sensitive areas.
I. Introduction

II. Theory of laser fault injection
   Physics and basics of laser fault injection
   Fault models of LFI

III. Static LFI experimental results
    Setup, results, analysis

IV. Dynamic LFI experimental results
    Setup, results, analysis

V. Conclusion
II. Theory of laser fault injection

- Fault model: mathematical expression at bit level
  - bit-flip (usual fault model, data independent)
    
    $$ b \rightarrow \text{not}(b) $$
II. Theory of laser fault injection

- Fault model: mathematical expression at bit level
  - bit-set/reset fault model (data dependent)
    
    \[
    \begin{align*}
    \text{if } b = 0 & \rightarrow \boxed{b = 1} \\
    \text{if } b = 1 & \rightarrow b = 1
    \end{align*}
    \]

    \[
    \begin{align*}
    \text{if } b = 0 & \rightarrow b = 0 \\
    \text{if } b = 1 & \rightarrow \boxed{b = 0}
    \end{align*}
    \]

- Provide additional information on the original bit value
  - Safe error attack (e.g. retrieving memory bits)
II. Theory of laser fault injection

- bit-set/reset fault model: D latch layout vs. laser effect area

Laser sensitive areas:
- SEU sensitive for $Q = 1$
- SEU sensitive for $Q = 0$

Laser spot size/effect area:

One laser sensitive area exposed

bit-set/reset fault model
II. Theory of laser fault injection

- bit-set/reset fault model: Dff layout vs. laser effect area

Laser sensitive areas:
- SEU sensitive for Q = 1
- SEU sensitive for Q = 0

Laser spot size/effect area:

Overlaps of laser sensitive areas

bit-flip fault model
II. Theory of laser fault injection

- Experimental state of the art
  - 2015, B. Selmke et al.: 45 nm SRAM (FPGA)
  - 2015, C. Champeix et al.: 40 nm D flip-flop
  - Both consistent with single-bit and bit-set/reset fault models

Illustration for D flip-flop:
- 4 SEU sensitive areas of master latch (clk = 1),
- 3 SEU sensitive areas of slave latch (clk = 0).

B. Selmke et al., “Precise laser fault injections into 90 nm and 45 nm sram-cells,” CARDIS 2015.
I. Introduction

II. Theory of laser fault injection
   Physics and basics of laser fault injection
   Fault models of LFI

III. Static LFI experimental results
   Setup, results, analysis

IV. Dynamic LFI experimental results
   Setup, results, analysis

V. Conclusion
III. Static LFI experimental results

- Experimental setup
Experimental setup

- Backside injection
- Pulse width: 30 ps
  - up to 100 nJ
- Wavelength: 1,030 nm
- Pulse width: ns
  - 5-50 ns, max. power 1 W
  - 50 ns – 1 s, max. power 3 W
- Wavelength: 1,064 nm
- Spot size: 1 µm or 5 µm
III. Static LFI experimental results

- Experiments description

Laser head

Laser fault sensitivity maps drawing (colors according to the fault model)
III. Static LFI experimental results

- Custom D flip-flop registers, CMOS 28 nm
III. Static LFI experimental results

- Custom D flip-flop registers, CMOS 28 nm
  - Matrix shaped shift register with 64 D flip-flops

- DFF: ~ 40 transistors,
- large output buffer
III. Static LFI experimental results

- Custom D flip-flop registers, CMOS 28 nm
  - spot 1 µm / 30 ps / 0.5 nJ / Δxy = 1 µm / backside

![Diagram of flip-flop registers with labels for bit reset (1 → 0) and slave latch (clk = 0)]
III. Static LFI experimental results

- Custom D flip-flop registers, CMOS 28 nm
  - 3D view at 1 nJ
III. Static LFI experimental results

- Custom D flip-flop registers, CMOS 28 nm
  - in-line shift register with 10 D flip-flops
Custom D flip-flop registers, CMOS 28 nm
- spot 1 $\mu$m / 30 ps / 0.5 nJ / $\Delta xy = 0.2$ $\mu$m / backside

III. Static LFI experimental results
Memory elements, static test – Conclusion

Bit-set/reset fault model = relevant

Single-bit fault model experimentally assessed with a laser at the CMOS 28 nm node for 1 µm and 5 µm (see table below) laser spots.

<table>
<thead>
<tr>
<th>Energy [nJ]</th>
<th>0.4</th>
<th>0.5</th>
<th>0.8</th>
<th>1</th>
<th>1.5</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td># of faults</td>
<td>1</td>
<td>8</td>
<td>21</td>
<td>23</td>
<td>24</td>
<td>24</td>
<td>26</td>
<td>30</td>
<td>31</td>
</tr>
<tr>
<td># of 1-bit faults</td>
<td>1</td>
<td>8</td>
<td>15</td>
<td>17</td>
<td>10</td>
<td>7</td>
<td>7</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td># of 2-bit faults</td>
<td>-</td>
<td>-</td>
<td>6</td>
<td>6</td>
<td>7</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td># of 3-bit faults</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>4</td>
<td>7</td>
<td>8</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td># of 4-bit faults</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td># of 5-bit faults</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td># of 6-bit faults</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td># of 7-bit faults</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td># of 8-bit faults</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
I. Introduction

II. Theory of laser fault injection
   Physics and basics of laser fault injection
   Fault models of LFI

III. Static LFI experimental results
   Setup, results, analysis

IV. Dynamic LFI experimental results
   Setup, results, analysis

V. Conclusion
IV. Dynamic LFI experimental results

- Test chips CMOS 28 nm
  - Target: AES implementation (with parity-based CM, 100 MHz)
  - IR microphotography (rear side), obj. x20
Experimental setup

- Backside injection
- Pulse width: 30 ps
  - up to 100 nJ
- Wavelength: 1,030 nm
- Pulse width: ns
  - 5-50 ns, max. power 1 W
  - 50 ns – 1 s, max. power 3 W
- Wavelength: 1,064 nm
- Spot size: 1µm or 5 µm
IV. Dynamic LFI experimental results

- Hardware AES-128, CMOS 28nm, Vdd = 1.2V, 100MHz
  - Exp.: 5 µm spot, 10 ns, 0.6-1.0 W, $\Delta xy = 1\mu m$
  - 26,380 faulted cipher texts
    - Unidentified faults: 6,574 (24.9 %)
      - mainly 5 – 8 faulty bytes (up to 12)
    - Identified faults: 19,806
      - single-byte faults
IV. Dynamic LFI experimental results

- **Hardware AES-128, CMOS 28nm, Vdd = 1.2V, 100MHz**
  
  Exp.: 5 µm spot, 10 ns, 0.6-1.0 W, $\Delta xy = 1\mu m$

---

Single-byte faults analysis

<table>
<thead>
<tr>
<th># faulted bits</th>
<th>Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>19,413</td>
</tr>
<tr>
<td>2</td>
<td>278</td>
</tr>
<tr>
<td>3</td>
<td>27</td>
</tr>
<tr>
<td>4</td>
<td>48</td>
</tr>
<tr>
<td>5</td>
<td>38</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

Exp. single-bit LFI rate: 73.6 %
I. Introduction

II. Theory of laser fault injection
   Physics and basics of laser fault injection
   Fault models of LFI

III. Static LFI experimental results
   Setup, results, analysis

IV. Dynamic LFI experimental results
   Setup, results, analysis

V. Conclusion
Exp. LFI fault model analysis at CMOS 28 nm

- **Single-bit**: static & dynamic tests (~70% success rate)
  - 1 μm & 5 μm laser spot size
  - ps & ns laser pulse duration

- **Data dependence**: bit-set/reset on D flip-flops
  - well defined sensitive areas

Single-bit & Bit-set/reset are still actual and practical fault models at advanced CMOS technology nodes (28 nm).

Q? Does it still holds at the CMOS 14 nm node?
Thank you for your attention
dutertre@emse.fr

Work funded by the ANR: LIESSE project
ANR-12-INS-0008-01

J.M. Dutertre¹, V. Beroulle², P. Candelier³, S. De Castro¹,⁴, L.B. Faber³, M.L. Flottes⁴, P. Gendrier³, D. Hély², R. Leveugle⁵, P. Maistri⁵, G. Di Natale⁴, A. Papadimitriou², B. Rouzeyre⁴

(1) MINES Saint-Étienne
(2) LCIS
(3) LIRMM
(4) LIFEA
(5) TIMA