Fault Model Analysis of Laser-Induced Faults in SRAM Memory Cells

Cyril Roscian, Alexandre Sarafianos, Jean-Max Dutertre, Assia Tria

Secured Architecture and System Laboratory – Centre Microélectronique de Provence - Gardanne
• Faults are often modeled according to two fault models:
  • Bit Set (resp. Reset)
  • Bit Flip

• Not much analysis on the fault model in SRAM:
  • Faults type
  • Effects of the fault injection on the SRAM

→ Analyze the fault model on SRAM memory cell
• Introduction
  • Fault model
  • Fault injection mechanism
  • Sensitivity zones
• Experiments on the SRAM cell
  • Sensitivity map
  • Spice Simulations
• Experiments on microcontroller RAM memory
  • Sensitivity map
• Conclusion & Perspectives
Bit set (resp. reset)

- Its value is changed: ‘0’ => ‘1’ (resp. ‘1’ => ‘0’)
- Result in a calculation error
- Unfaulted if its value was already ‘1’ (resp. ‘0’)
- **Allow to mount safe error attacks**

Bit flip

- Independent of the data value (‘0’ => ‘1’ or ‘1’ => ‘0’)
- Induces a calculation error
- Better fault injection rate
- Quicker analysis of the faulted results
Fault injection mechanism

- Creation of electron-hole pair along the laser beam due to the photoelectric effect
- Stretch the electric field
- Creation of a transient current
- Possible SEE on PN junction
  - Source and drain of transistors
Sensitivity zones

- Inverter’s case:
  - 1st Case (output = ‘1’)
    - PMOS ON
    - NMOS OFF
    - Only a strike on drain of NMOS will discharge the load and change the output state

The sensitivity zone is the drain of the OFF NMOS transistors
Sensitivity zones

- Inverter’s case:
  - 2\textsuperscript{st} Case (output = ‘0’)
    - PMOS OFF
    - NMOS ON
    - Only a strike on drain of PMOS will charge the load and change the output state

The sensitivity zone is the drain of the OFF PMOS transistors
• Configuration SRAM (programmable logic)
  • 5 transistors

• 0.25µm CMOS Technology

• Size: 9µm x 4µm
Experimental setup

- Front side fault injection
- 1064nm wavelength
- Spot size: 1μm
- Pulse duration: 50 ns
- Energy from 1W to 1.6W
- SRAM grid pattern: 0.2μm
Sensitivity zones

- 4 theoretical zones
  - Corresponding to the drain of the OFF transistors
- 2 zones when \textit{DATA\_OUT} is in high state
- 2 zones when \textit{DATA\_OUT} is in low state

Bit Set zones

Bit Reset zones
Sensitivity zones

- Laser spot size of 1µm
- Sensitivity zones extended
- Bit set and reset zones overlap
- For some positions: faults injected should be bit flip
Sensitivity map of the memory cell

- Red zone and blue zone do not overlap.
- **No bit flip**
- Only 3 zones are really sensitive.

- **SPICE simulation on the edge zone**
Based on the model of Sarafianos et al.[1]
- Model developed with 90nm CMOS technology
- Using Voltage controlled current source
- Multiple current sources (several sensitive zones)

The laser beam can reach several sensitivity zones of the cell

First simulation

- Similar to the experiments
- Same hidden zone
- No bit flip
- Simulations on the Bit-set position
Simulation of Bit-set fault

- Current injected on the drain of MN2
- Current of MP2 in opposition
- State has already changed
- Fault is injected (Bit-set)
Simulation of Bit-reset fault

- Current injected in drain of MN1
- Two other current are in opposition
- No fault injected
• No bit flip
  • Despite the laser beam effect zone (Ø 1μm & 5μm)
  • Energy between 1W and 1.6W
  • Balanced current that avoid fault

• Confirmation of these results with microcontroller RAM memory
  • Several memory cells
  • Different technology
  • SRAM with 6 transistors
Experimental setup

- 8-bits microcontroller
- CMOS 0.35\(\mu\)m technology
- 4kB divided on 8 parts
  - Each part contains 2 blocks of 256 Bytes
- Zone of 40 x 40 \(\mu\)m\(^2\) used
Experimental setup

- 6 transistors SRAM cell
  - 4 theoretical sensitivity zones
  - 2 Bit-set zones
  - 2 Bit-reset zones
- Spot size of 1µm & 5µm
- Power of 1.1W & 1.2W
Sensitivity map with $\phi 1\mu m$ and 1.1W

- 12 memory cells identified
  - Size approx. $5 \times 5 \mu m^2$
- No Bit-flip
- Only 2 sensitivity zones
  - 4 theoretical zones
Sensitivity map with $\Ø5\mu$m and 1.1W

- No memory cells identified
- No Bit-flip
- Spot size has no effect on the injection of Bit-flip fault
• No Bit-flip
  • Balanced current that avoid fault
  • Same behavior with different SRAM cells
  • Bit-flip fault model is not the most relevant model
  • Allow to mount safe error attack on microcontroller RAM

• Futur works
  • Countermeasures will be investigated using the hidden zone
  • Laser fault injection with pico-seconds laser pulse
Thank you for your attention.

Questions?

Acknowledgment: The research work of Cyril Roscian was partly funded by the ‘Conseil Régional Provence-Alpes Côte d’Azur’