Laser Fault Injection into SRAM cells: Picosecond versus Nanosecond pulses

Marc Lacruche*, Nicolas Borrel†, Clement Champeix*†, Cyril Roscian*, Alexandre Sarafianos†, Jean-Baptiste Rigaud*, Jean-Max Dutertre*, Edith Kussener‡

* École Nationale Supérieure des Mines de Saint-Étienne,
† ST Microelectronics,
‡ IM2NP
Outline

• Context
• Laser fault injection
• Previous works: 50ns pulses
• 30ps pulses
• Simulation model upgrade
• Commercially available product validation
• Conclusion
Context

- **Security point of view**: ns or µs pulses are generally used
  - Are ps pulses used in radiative works valid for security testing?

- **Fault Attacks**
  - Disturb a circuit during computations
  - Exploit resulting computation errors
    - Retrieve encryption keys

  - **Differential Fault Analysis (DFA)**
    - “On the importance of checking cryptographic protocols for faults”, D. Boneh, R. A. DeMillo, and R. J. Lipton, EUROCRYPT’97

  - Fault Model choice critical for the success of the attack.
Laser Fault Injection

- Photoelectric Effect:
Laser Fault Injection

• Gate Level
Laser Fault Injection

• Transistor Level
  – 5T SRAM
Laser Fault Injection

• Layout Level

Bit-Flips?

Bit-Set Sensitive Area
Bit-Reset Sensitive Area
Previous Works: 50ns Pulses

• “Fault model analysis of laser-induced faults in sram memory cells”, C. Roscian, A. Sarafianos, J.-M. Dutertre, and A. Tria FDTC 2013

• Test Setup:
  – Test Chip: 5 Transistor SRAM Cell
    • Technology: 0.25 µm
    • Cell size: 4µm x 9µm
    • Few metal layers to allow front side injection
  – Laser Setup
    • Wavelength: 1064nm
    • Spot size: 1µm
    • Laser Power: 0.42W
    • Pulse Duration: 50ns
    • Frontside Injection
Previous Works: 50ns Pulses

- Experimental Results: Single SRAM Cell

  - No fault induced in the MP2 drain area
  - No Bit-Flips at the limit between MN1 and MN3
Previous Works: 50ns Pulses

• Simulation Results: Single SRAM Cell

• Electrical simulation model takes the cell layout into account

• Area masking caused by a counter-balancing effect in the shared drain of MN3 and MN2
30ps Pulses

• Laser Setup
  – Wavelength: 1064nm
  – Spot size 1µm
  – Laser energy: 3.2nJ
  – Pulse duration: 30ps

• Same 5 Transistor SRAM Chip as the 50ns tests

• Is the Bit-Set/Bit-Reset model still valid over the Bit-Flip one?
• Is the area-masking still in effect?
30ps Pulses

- Experimental Results: Single SRAM Cell

  Faults appear when targeting the MP2 Drain
  Still no Bit-Flip positions
Simulation Model Adaptation

- “Building the electrical model of the pulsed photoelectric laser stimulation of an nmos transistor in 90nm technology”, A. Sarafianos, O. Gagliano, V. Serradeil, M. Lisart, J.-M. Dutertre, and A. Tria, IRPS 2013

\[ I_{ph}(t) = [a(E) \cdot V_r + b(E)] \cdot A \cdot \alpha_{topology} \cdot \Omega_{shape}(t) \]

- \( a(E) \) and \( b(E) \): Experimental coefficients depending on laser energy \( E \)
- \( V_r \): Junction reverse voltage
- \( A \): Junction area
- \( \alpha_{topology} \): Laser beam spatial intensity profile
- \( \Omega_{shape}(t) \): Laser pulse temporal shape
Simulation Model Adaptation

• Hypothesis:
  – 30ps pulses have a reduced effect area
  • Adjusted $\alpha_{topology}$ coefficient:

![Graph showing measurement and extrapolation](image)
Simulation Model Adaptation

- Simulation Results: SRAM Cell (30ps Pulses)
  - 4 Sensitive Areas
  - No bit-flip
  - Metal layers not taken into account
  - Areas shapes differ
Commercially Available Product Validation

- Microcontroller RAM: Previous 50ns results
  - 0.35µm technology
  - Same Laser Settings
  - 6 Transistor Cells
  - Backside Injection
  - Still no bit-flip
  - 2 Masked Areas per Cell
Commercially Available Product Validation

- Microcontroller RAM: 30ps results
  - Same Laser Settings
  - Same Microcontroller as the 50ns tests
  - Still no bit-flip
  - 4 areas per cell
Conclusion

• Limiting testing to nanosecond range pulses may hide vulnerabilities
  – Test using varying pulse lengths as consequence
• Bit-set/bit-reset model still valid over Bit-flip model
• Simulation model extended for 30ps pulses

• Next Steps:
  – Finer 30ps simulation model tuning (Experimental)
  – Reproduce experimentations on more recent technologies
Thank you for your attention.
Simulation Model Details

[Diagram with nodes labeled Vdd, Gnd, Sel, Data_in, and Data_out, showing a circuit with transistors and connecting lines.]