Importance of IR Drops on the Modeling of Laser-Induced Transient Faults

Raphael Viera, Philippe Maurine, Jean-Max Dutertre and Rodrigo Bastos
Importance of IR Drops on the Modeling of Laser-Induced Transient Faults

Raphael Viera, Philippe Maurine, Jean-Max Dutertre and Rodrigo Bastos
Outline

1. Motivation
2. Classical model of laser fault injection and its limits
3. Proposed model
4. Simulation methodology
5. Simulation results
6. Conclusions
1 Motivation

2 Classical model of laser fault injection and its limits

3 Proposed model

4 Simulation methodology

5 Simulation results

6 Conclusions
Many Smart Cards among us nowadays
Many Smart Cards among us nowadays

Credit/Debit Card  Passport  Company Badge

Health Insurance  ID Card  Phone SIM Card

And more...
Smart Card is not only a data storage
**Smart Card** is not only a data storage

It's a secure **microcontroller**
**Smart Card** is not only a data storage

It's a secure **microcontroller**

**Encryption** algorithms such as AES, DES, 3DES, RSA and ECC
Smart Card is not only a data storage

It's a secure microcontroller

Encryption algorithms such as AES, DES, 3DES, RSA and ECC

Fault-based attack to extract confidential data
Smart Card is not only a data storage

It's a secure microcontroller

Encryption algorithms such as AES, DES, 3DES, RSA and ECC

Fault-based attack to extract confidential data

How to attack?
Laser based attack.
Laser based attack.

Effective and accurate fault injection tool
Laser-based attack.

How to defend?

Effective and accurate fault injection tool
Laser based attack.

How to defend?

- Detection
- Design robust circuits

Effective and accurate fault injection tool
Laser based attack.

**How to defend?**

- Detection
- Design robust circuits

Simulate the effects of laser shots on ICs

Effective and accurate fault injection tool
Laser based attack.

Effective and accurate fault injection tool

How to defend?

Detection
Design robust circuits

Simulate the effects of laser shots on ICs

Importance of having accurate laser-fault injection models
Laser-induced transient fault model with IR-drop contribution
Paper Contributions

- Laser-induced transient fault model with IR-drop contribution
- Methodology to simulate the effects of laser shots on ICs
Paper Contributions

- Laser-induced \textit{transient fault model} with IR-drop contribution
- \textbf{Methodology} to simulate the effects of laser shots on ICs
- Analyse the impact of laser-induced \textit{IR-drop} in the fault injection process
1. Motivation
2. Classical model of laser fault injection and its limits
3. Proposed model
4. Simulation methodology
5. Simulation results
6. Conclusions
Outline

1 Motivation

2 Classical model of laser fault injection and its limits

3 Proposed model

4 Simulation methodology

5 Simulation results

6 Conclusions
Classical model for simulating laser-induced transient currents on ICs
Classical model for simulating laser-induced transient currents on ICs
Classical model for simulating laser-induced transient currents on ICs

Sensitive areas (reverse biased PN junction between the drain and the substrate)
Spatial distribution of the laser-induced photocurrent

\[ I_{ph} = (a \times V + b) \times \alpha_{gauss(x,y)} \times Pulse_w \times S \]

A. Sarafianos et al., “Building the electrical model of the pulsed photoelectric laser stimulation of an nmos transistor in 90nm technology”
Spatial distribution of the laser-induced photocurrent

\[ I_{ph} = (a \times V + b) \times \alpha_{gauss(x,y)} \times Pulse_w \times S \]

A. Sarafianos et al., “Building the electrical model of the pulsed photoelectric laser stimulation of an nmos transistor in 90nm technology”
Spatial distribution of the laser-induced photocurrent

\[ I_{ph} = (a \times V + b) \times \alpha_{gauss}(x,y) \times Pulse_w \times S \]

A. Sarafianos et al., “Building the electrical model of the pulsed photoelectric laser stimulation of an nmos transistor in 90nm technology”
Standard cell(s) illuminated by a 5μm laser spot diameter

tech: 250 nm

12.5 μm
Standard cell(s) illuminated by a 5μm laser spot diameter
Standard cell(s) illuminated by a 5μm laser spot diameter
Standard cell(s) illuminated by a 5μm laser spot diameter

How does the standard cell height influence in the fault injection process?
Case 1:
Only NMOS transistors are illuminated by the laser beam

- Classical model of laser fault injection and its limits

2.2 - Limits of the classical transient fault model

- Tech: 250 nm
- Load: '0', '1'
- Width: 12.5 μm
Case 1:
Only NMOS transistors are illuminated by the laser beam
Case 1:
Only NMOS transistors are illuminated by the laser beam

No laser-induced currents in the Nwell-Psub junction (classical model is OK)
Case 2:

NMOS and PMOS transistors are illuminated by the laser beam
Case 2:

NMOS and PMOS transistors are illuminated by the laser beam.
Case 2:

NMOS and PMOS transistors are illuminated by the laser beam

Laser-induced currents in the Nwell-Psub junction (classical model is **incomplete**)

**tech:** 250 nm

**Pload**

'0' > '1'
Case 3:
Only PMOS transistors are illuminated by the laser beam
Case 3:
Only PMOS transistors are illuminated by the laser beam
Case 3:
Only PMOS transistors are illuminated by the laser beam

Laser-induced currents in the Nwell-Psub junction (classical model is **incomplete**).
Case 4:
NMOS and PMOS transistors are always illuminated by the laser beam.
Case 4:
NMOS and PMOS transistors are always illuminated by the laser beam.
**Case 4:**
NMOS and PMOS transistors are always illuminated by the laser beam.

Laser-induced currents in the Nwell-Psub junction (classical model is incomplete).
1 Motivation
2 Classical model of laser fault injection and its limits
3 Proposed model
4 Simulation methodology
5 Simulation results
6 Conclusions
Outline

1 Motivation
2 Classical model of laser fault injection and its limits
3 Proposed model
4 Simulation methodology
5 Simulation results
6 Conclusions
3.1 - Upgraded electrical model

Classical Model

Upgraded Electrical Model
3 - Proposed model

3.1 - Upgraded electrical model

Classical Model

Upgraded Electrical Model
3.1 - Upgraded electrical model

Classical Model

Upgraded Electrical Model

\[ I_{ph} = (a \times V + b) \times \alpha_{gauss}(x,y) \times Pulse_w \times S \]

\[ IP_{Psub_nwell} = factor \times I_{ph} \]
Classical Model

Upgraded Electrical Model

\[ I_{ph} = (a \times V + b) \times \alpha_{gauss}(x,y) \times Pulse_w \times S \]

\[ IP_{P_{sub \_nwell}} = \text{factor} \times I_{ph} \]

J.M. Dutertre et al., “Improving the ability of Bulk Built-In Current Sensors to detect Single Event Effects by using triple-well CMOS”
1. Motivation
2. State of the art of laser fault injection and limits of the classical approach
3. Proposed model and its consequences on the fault injection mechanism
4. Simulation methodology
5. Simulation results
6. Conclusions
1. Motivation
2. State of the art of laser fault injection and limits of the classical approach
3. Proposed model and its consequences on the fault injection mechanism
4. Simulation methodology
5. Simulation results
6. Conclusions
5.0 - Case study

ARM 7 processor
CMOS 28 nm
VDD = 1 V
110 μm x 70 μm
Laser spot diameter = 5 μm
Set the amplitude of the exponential currents according to:

\[ I_{ph} = (a \times V + b) \times \alpha_{gauss}(x, y) \times Pulse_{w} \times S \]

\[ IP_{Sub\_nwell} = factor \times I_{ph} \]
5.1 - Maximum Voltage Drop Propagation

Without laser illumination
5 - Simulation Results

5.1 - Maximum Voltage Drop Propagation

Without laser illumination

With laser illumination

Voltage swing = 209 mV
5.1 - Maximum Voltage Drop Propagation

Without laser illumination

With laser illumination

Voltage swing = 209 mV
5.1 - Maximum Voltage Drop Propagation

Without laser illumination

With laser illumination

Voltage swing = 209 mV

Time = 1.55 ns  Time = 1.6 ns  Time = 1.7 ns  Time = 2.0 ns  Time = 2.4 ns  Time = 2.8 ns
5 - Simulation Results

5.2 - Simulated Scenarios and Fault Injection Maps

Data_out<\textcolor{red}{x}>, Addr_out<\textcolor{red}{x}>, Etc_out<\textcolor{red}{x}>

Volts

Time (ns)

0 0.5 1 1.5 2 2.5 3

Fault at 1.5 ns

Fault at 1.7 ns

Fault at 1.9 ns

Simulations using only IPh current component

\text{Xaxis (\textmu m)}

\text{Yaxis (\textmu m)}

\text{Volts}

\text{CLK}

\text{D<\textcolor{red}{x}>}

\text{Volts}

\text{PU} \quad \text{IPh} \quad \text{Y}

\text{PD} \quad \text{IPh} \quad \text{CLoad}
5 - Simulation Results

5.2 - Simulated Scenarios and Fault Injection Maps

[Diagrams and graphs showing voltage levels and timing data for various scenarios, including circuit diagrams and micrographs of cell X and Y.]
5.2 - Simulated Scenarios and Fault Injection Maps

![Simulation Results Diagram]

- **5.2 - Simulated Scenarios and Fault Injection Maps**

![Volts and Time Graph]

- **5.2 - Simulated Scenarios and Fault Injection Maps**

![Simulation Circuits]

- **5.2 - Simulated Scenarios and Fault Injection Maps**
5.2 - Simulated Scenarios and Fault Injection Maps

![Diagram of ARM7 Cell X and associated waveforms and circuitry]
5.2 - Simulated Scenarios and Fault Injection Maps

The diagrams and graphs illustrate the simulation results for various scenarios and fault injections. The first graph shows the timing of events over time (ns), with voltage levels indicated for ARM7, Cell X, Data_out<x>, Addr_out<x>, Etc_out<x>, and D<x>. The second graph presents fault scenarios at 1.5 ns, 1.7 ns, and 1.9 ns, respectively, with visualizations of the affected areas on the chip. The circuit diagram at the bottom left represents the components involved in the simulations: PU, IPh, PD, C_load, X, Y, and IPh current component.
5 - Simulation Results

5.2 - Simulated Scenarios and Fault Injection Maps

Images and graphs showing various scenarios and fault injection maps for different time points and components within the system.
5 - Simulation Results

5.2 - Simulated Scenarios and Fault Injection Maps

Volts

Time (ns)

0 0.5 1 1.5 2 2.5 3

Data_out<x>
Addr_out<x>
Etc_out<x>

Fault at 1.5 ns
Fault at 1.7 ns
Fault at 1.9 ns

Simulations using only IPh
Simulations using only IPsub_nwel

Power grid model

PU
IPh
X
Y
PD
IPh
X
Y

Power grid model

CLoad
5 - Simulation Results

5.2 - Simulated Scenarios and Fault Injection Maps

![Image of ARM7 cell X with voltage and time plots]

- **Volts**
- **Time (ns)**
- **Data_out<->**
- **Addr_out<->**
- **Etc_out<->**

---

![Image of voltage and current component simulations]

- **Simulations using only IPh current component**
- **Simulations using only IPhsub_nwell**
- **Simulations using IPh + IPhsub_nwell**

---

![Image of power grid model]

- **Power grid model**
- **IPh**
- **IPhsub_nwell**
- **C_Load**

---
5.3 - IR drop contribution to the fault injection mechanism

\[
\Delta V_{out\ (without\ IR)} = - \frac{I_{PhNMOS}}{\mu \cdot C_{ox} \cdot W} (V_{DD} - V_T)
\]
5.3 - IR drop contribution to the fault injection mechanism

\[ \Delta V_{out\,(without IR)} = - \frac{I_{PhNMOS}}{\mu \cdot C_{ox} \cdot W} (V_{DD} - V_T) \]

\[ \Delta V_{out\,(with IR)} = - V_{drop} - \frac{I_{PhNMOS}}{\mu \cdot C_{ox} \cdot W} (V_{DD} - V_{drop} - V_T) \]
5.3 - IR drop contribution to the fault injection mechanism

\[ \Delta V_{\text{out}}(\text{without IR}) = - \frac{I_{\text{PHNMOS}}}{\mu \cdot C_{\text{ox}} \cdot W} (V_{\text{DD}} - V_T) \]

\[ \Delta V_{\text{out}}(\text{with IR}) = - V_{\text{drop}} - \frac{I_{\text{PHNMOS}}}{\mu \cdot C_{\text{ox}} \cdot W} (V_{\text{DD}} - V_{\text{drop}} - V_T) \]
5 - Simulation Results

5.3 - IR drop contribution to the fault injection mechanism

\[
\Delta V_{out\ (without IR)} = - \frac{I_{PhNMOS}}{L} \frac{\mu \cdot C_{ox} \cdot W}{V_{DD} - V_T} \nabla V_{drop}
\]

\[
\Delta V_{out\ (with IR)} = - V_{drop} - \frac{I_{PhNMOS}}{L} \frac{\mu \cdot C_{ox} \cdot W}{V_{DD} - V_{drop} - V_T}
\]

\[
\frac{\Delta V_{out\ (with IR)}}{\Delta V_{out\ (without IR)}} = 1 - \frac{V_{drop}}{V_{DD} - V_T}
\]
1 Motivation
2 Classical model of laser fault injection and its limits
3 Proposed model
4 Simulation methodology
5 Simulation results
6 Conclusions
Outline

1. Motivation
2. Classical model of laser fault injection and its limits
3. Proposed model
4. Simulation methodology
5. Simulation results
6. Conclusions
Conclusions

IPpsub_nwell current component is always present (causing IR-drops)
Conclusions

IPpsub_nwell current component is always present (causing IR-drops)
Conclusions

**IPpsub_nwell current component is always present (causing IR-drops)**

Ignoring the laser-induced IR drop may result in underestimating the risk of fault injection
Conclusions

**IPpsub_nwell** current component is always present (causing IR-drops)

Ignoring the laser-induced IR drop may result in underestimating the risk of fault injection.
Ipps sub nwell current component is always present (causing IR-drops)

Ignoring the laser-induced IR drop may result in underestimating the risk of fault injection

Methodology to simulate the effects of laser shots on ICs based on standard CAD tools
Importance of IR Drops on the Modeling of Laser-Induced Transient Faults

Raphael Viera, Philippe Maurine, Jean-Max Dutertre and Rodrigo Bastos
Appendix
Case 4:
Both NMOS and PMOS transistors are illuminated by the laser beam

Laser-induced currents in the Nwell-Psub junction (classical model is incomplete)
Case 6:
NMOS and PMOS transistors are always illuminated by the laser beam

Laser-induced currents in the Nwell-Psub junction (classical model is incomplete)
Run a fault free electrical simulation

Save a golden table with all inputs and outputs of each cell as a function of time

Upgraded model still not in use
3.2 - Influence of the IPh current component

(a)

(b)

(c)

<table>
<thead>
<tr>
<th>Time</th>
<th>1ns</th>
<th>1.2</th>
<th>1.4</th>
<th>1.6</th>
<th>1.8</th>
<th>2ns</th>
<th>2.2</th>
<th>2.4</th>
<th>2.6</th>
<th>2.8</th>
<th>3ns</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLK tsetup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLK thold</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLK TCLK</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Di</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qi</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tclk2Q Qi</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tQ2Do Do</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qo</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tclk2Q Qo</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Soft Error
3.3 - Influence of the IPPsub_nwell current component
3.4 - Influence of IPh and IPPsub_nwel current components

(a) Diagram showing non-ideal VDD and GND connections.

(b) Diagram showing IPh and IPPsub_nwel connections.

(c) Time table showing setup, hold, and TCLK times.
5.3 - IR drop contribution to the fault injection mechanism

\[ \Delta V_{\text{out (without IR)}} = -\frac{I_{\text{PhNMOS}}}{\mu C_{\text{ox}} W} (V_{DD} - V_T) \]
5 - Simulation Results

5.3 - IR drop contribution to the fault injection mechanism

\[ \Delta V_{out}(without IR) = - \frac{I_{PhNMOS}}{L \cdot \mu \cdot C_{ox} \cdot W} (V_{DD} - V_T) \]

\[ \Delta V_{out}(with IR) = - V_{drop} - \frac{I_{PhNMOS}}{L \cdot \mu \cdot C_{ox} \cdot W} (V_{DD} - V_{drop} - V_T) \]
5.3 - IR drop contribution to the fault injection mechanism

\[ \Delta V_{out}(\text{without IR}) = - \frac{I_{PhNMOS}}{\mu C_{ox} W L} (V_{DD} - V_T) \]

\[ \Delta V_{out}(\text{with IR}) = - V_{drop} - \frac{I_{PhNMOS}}{\mu C_{ox} W L} (V_{DD} - V_{drop} - V_T) \]
5 - Simulation Results

5.3 - IR drop contribution to the fault injection mechanism

\[ \Delta V_{out\ (without\ IR)} = -\frac{I_{Ph_{NMOS}}}{\mu \cdot C_{ox} \cdot W (V_{DD} - V_T)} \]

\[ \Delta V_{out\ (with\ IR)} = -V_{drop} - \frac{I_{Ph_{NMOS}}}{\mu \cdot C_{ox} \cdot W (V_{DD} - V_{drop} - V_T)} \]

\[ \frac{\Delta V_{out\ (with\ IR)}}{\Delta V_{out\ (without\ IR)}} = 1 - \frac{1}{\frac{V_{drop}}{V_{DD} - V_T}} \]
5.5 - Total dynamic current flowing in the circuit

(a) Without laser spot - VDD

(b) Without laser spot - GND

(c) 5µm laser spot - VDD

(d) 5µm laser spot - GND
5.5 - Total dynamic current flowing in the circuit

More than 25 mA of induced current distributed among hundreds of standard cells

Around 200 uA per cell in the epicentre
5 - Simulation Results

5.4 - Probability of soft error occurrence

- **Shot_t**: Laser shot time
- **IPh**: IPh contribution only
- **IPh + IPsub**: IPh + IPsub_nwell contribution

### Diagram

- **CLK**
- **IPh**
- **IPh + IPsub**

Path X is represented by blue lines, and Path Y is represented by red lines.

The probability of soft error occurrence is shown with respect to time, with specific intervals marked for analysis.