Frontside Laser Fault Injection on Cryptosystems
-Application to the AES’s last round-

Cyril Roscian, Jean-Max Dutertre and Assia Tria

Secured Architecture and System Laboratory – Centre Microélectronique de Provence - Gardanne
Planning

- Introduction
  - Laser effect on ICs
  - Sensitivity zones
  - Fault injection mechanism
- Experimental Setup
- Analysis of fault injection
- Performing DFA on experimental data
  - Giraud’s DFA
  - Roche et al. DFA
  - Simplification of existing DFA
- Conclusion
Laser effect on ICs

- 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:
  - 1\textsuperscript{st} 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:
  - 2nd 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
Fault injection mechanism

- SET reaches the DFF’s input outside the latching window
  - No effect on the DFF’s output
  - No fault on the computational results
Fault injection mechanism

- SET reaches the DFF’s input inside the latching window
- DFF’s output is changed
- A fault occurred on the computational results
Fault injection mechanism

- SET reaches the DFF itself or an SRAM
  - Memory constructed with cross-coupled inverter
  - The SET will propagate through the inverters
  - The memorized data is inverted
  - A fault is injected
Laser Fault model

- Laser spot strike one sensitive area
  - Fault data-dependent
  - Bit-Set/Bit-Reset fault model
  - Allow to mount safe error attacks
- Questionable with advanced CMOS IC
  - Smallest laser spot of 1µm
  - Several transistors reaches by the spot
  - Impact of metal layers
Laser Fault model

- Possible Bit-flip
- Most of injection on rear side with small spot
  - Time consuming
  - Chip preparation
- Front side
  - Easy
  - But not consistent with bit-set/reset

- Investigation of fault type in front side with large spot
Laser test bench

- Front side fault injection
- Wavelength of 532nm
- Laser pulse of 5ns
- Square laser spot of $125\mu m \times 125\mu m$
- Energy density of $17\text{pJ}/\mu m^2$
- Laser shoot synchronized with AES encryption
  - Jitter of 5ns
  - Laser shoot during the last round of the AES
Target device

- Target device is an ASIC with implementation of the AES algorithm.
- 128 bits key length.
- One round executed in one clock cycle.
- All AES encryption executed on 11 clock cycle.
- Frequency of 25MHz.
- 0.13µm technology with 6 metal layers.
Fault injection on AES’ last round

- Surface of the chip divided on 36 positions
- 10,000 encryptions for each position
- Same key used for all encryption
- Comparison between faulted and correct cipher text
- Fault value recovered by reversing the faulted encryption (the key was known)
## Fault injection on AES’ last round

<table>
<thead>
<tr>
<th>byte #</th>
<th>Error injection rate</th>
<th>Single-bit error rate</th>
<th>Most common fault rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>4.8%</td>
<td>79%</td>
<td>74%</td>
</tr>
<tr>
<td>1</td>
<td>3.2%</td>
<td>100%</td>
<td>99%</td>
</tr>
<tr>
<td>2</td>
<td>3.1%</td>
<td>98%</td>
<td>92%</td>
</tr>
<tr>
<td>3</td>
<td>67.8%</td>
<td>49%</td>
<td>48%</td>
</tr>
<tr>
<td>4</td>
<td>9.4%</td>
<td>99.7%</td>
<td>90%</td>
</tr>
<tr>
<td>5</td>
<td>2.1%</td>
<td>79%</td>
<td>58%</td>
</tr>
<tr>
<td>6</td>
<td>0.5%</td>
<td>100%</td>
<td>99%</td>
</tr>
<tr>
<td>7</td>
<td>4.6%</td>
<td>65%</td>
<td>64%</td>
</tr>
<tr>
<td>8</td>
<td>23%</td>
<td>64%</td>
<td>42%</td>
</tr>
<tr>
<td>9</td>
<td>7.2%</td>
<td>91%</td>
<td>80%</td>
</tr>
<tr>
<td>10</td>
<td>4.3%</td>
<td>99%</td>
<td>98%</td>
</tr>
<tr>
<td>11</td>
<td>15.5%</td>
<td>97%</td>
<td>97%</td>
</tr>
<tr>
<td>12</td>
<td>12.2%</td>
<td>98%</td>
<td>96%</td>
</tr>
<tr>
<td>13</td>
<td>3.1%</td>
<td>87%</td>
<td>55%</td>
</tr>
<tr>
<td>14</td>
<td>0.2%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>15</td>
<td>7%</td>
<td>99.2%</td>
<td>99%</td>
</tr>
</tbody>
</table>
Fault injection on AES' last round

<table>
<thead>
<tr>
<th>byte #</th>
<th>Error injection rate</th>
<th>Single-bit error rate</th>
<th>Most common fault rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>4.8%</td>
<td>79%</td>
<td>74%</td>
</tr>
<tr>
<td>1</td>
<td>3.2%</td>
<td>100%</td>
<td>99%</td>
</tr>
<tr>
<td>2</td>
<td>3.1%</td>
<td>98%</td>
<td>92%</td>
</tr>
<tr>
<td>3</td>
<td>67.8%</td>
<td>49%</td>
<td>48%</td>
</tr>
<tr>
<td>4</td>
<td>9.4%</td>
<td>99.7%</td>
<td>90%</td>
</tr>
<tr>
<td>5</td>
<td>2.1%</td>
<td>79%</td>
<td>58%</td>
</tr>
<tr>
<td>6</td>
<td>0.5%</td>
<td>100%</td>
<td>99%</td>
</tr>
<tr>
<td>7</td>
<td>4.6%</td>
<td>65%</td>
<td>64%</td>
</tr>
<tr>
<td>8</td>
<td>23%</td>
<td>64%</td>
<td>42%</td>
</tr>
<tr>
<td>9</td>
<td>7.2%</td>
<td>91%</td>
<td>80%</td>
</tr>
<tr>
<td>10</td>
<td>4.3%</td>
<td>99%</td>
<td>98%</td>
</tr>
<tr>
<td>11</td>
<td>15.5%</td>
<td>97%</td>
<td>97%</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td></td>
<td>96%</td>
</tr>
<tr>
<td>13</td>
<td>3.1%</td>
<td></td>
<td>55%</td>
</tr>
<tr>
<td>14</td>
<td>0%</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>15</td>
<td>7%</td>
<td></td>
<td>99%</td>
</tr>
</tbody>
</table>

- Low Injection rate
- High repetitively rate
Fault injection on AES’ last round

- 1,000 encryption on byte #5

<table>
<thead>
<tr>
<th>Faults occurrence rate</th>
<th>Occurrence rate of fault ’0x80’</th>
<th>Occurrence rate of other faults</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1%</td>
<td>94%</td>
<td>6%</td>
</tr>
</tbody>
</table>

- Single bit fault of 0x80
- Faulted bit: “0” → “1”
- Bit-Set fault type
- If only Bit-Set fault is considered
  - From 7.4% to 14.2% occurrence rate
Fault injection on AES’ last round

- 1,000 encryption on byte #5 with chosen plain text

<table>
<thead>
<tr>
<th>Fault occurrence rate</th>
<th>Occurrence rate of fault ’0x80’</th>
<th>Occurrence rate of other faults</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.8%</td>
<td>97%</td>
<td>3%</td>
</tr>
</tbody>
</table>

- Timing constraint
  - Clock period of 40 ns
  - Jitter of 5 ns
- Bit-set fault model relevant
Fault injection on AES’ last round

- Analysis on byte #3
  - 34.2% fault occurrence on bit N° 2
  - 66% fault occurrence on bit N° 1
  - Bit N° 2 only impacted by Bit-Set fault type
  - Bit N° 1 impacted by Bit-flip fault type

- Some faulted bits are data-dependant

<table>
<thead>
<tr>
<th>Fault value</th>
<th># of occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000 0110</td>
<td>3285</td>
</tr>
<tr>
<td>0000 0010</td>
<td>3228</td>
</tr>
<tr>
<td>0000 1110</td>
<td>93</td>
</tr>
<tr>
<td>0000 1000</td>
<td>70</td>
</tr>
<tr>
<td>0000 0100</td>
<td>51</td>
</tr>
<tr>
<td>0000 0001</td>
<td>40</td>
</tr>
<tr>
<td>0000 1001</td>
<td>13</td>
</tr>
<tr>
<td>0000 0011</td>
<td>4</td>
</tr>
</tbody>
</table>
Fault injection on AES’ last round

- Bit-set/reset and Bit-flip fault model are relevant with large spot size and front side laser fault injection
- Metal fills act as shutter on laser beam
  - Hides some sensitive area
- Low injection rate but high repetitively of fault value
  - Comparison of two DFA schemes with these data
Giraud’s mono-bit

- Need a single bit fault injection on byte before the last round of the AES
- Success rate of 97% with 3 pairs of Correct/Faulted cipher text
- Only 3 bytes correspond with this statement
  - Bytes 1, 6 and 14
- 13 bytes are mono-bit occurrence close to 80%
  - Correct/Faulted cipher text needed increases
- 3 bytes close to 65% or above 50%
  - Not the most efficient schemes
Roche et al. DFA

- Need constant fault injection
- 3 pairs of Correct/Faulted cipher texts to have a success rate of 90%
- With our data:
  - 9 bytes need 6 or less pairs
  - 4 byte need at least 15 pairs
- More data needed to succeed compared to Giraud
- Fault model less constraining
Simplification of an existing DFA

- Byte-wise analysis of the error injected
- Equation of the AES’s last round for the correct and faulted ciphertext:

\[
C = K10 \oplus SB(M9) \\
D = SB(M9 \oplus e) \oplus K10
\]

- The equation of the error is:

\[
e = SB^{-1}(C \oplus K10) \oplus SB^{-1}(D \oplus K10)
\]

- For each pairs:
  - Computation of \( e \) for all possible \( K10 \)
  - Construction of an error table
Simplification of an existing DFA

- Simplification of an existing DFA
- Byte-wise analysis of the error injected
- Equation of the AES’s last round for the correct and faulted ciphertext:
  \[ e = SB^{-1}(C \oplus K10) \oplus SB^{-1}(D \oplus K10) \]

For each pair:
- Computation of \( e \) for all possible \( K10 \)
- Construction of an error table
Simplification of an existing DFA

- Only one column correspond to the right key hypothesis
- Visual discrimination between right and false hypothesis
- Easy to identify pattern from random value

- Only 3.5 faulted text with repeatability of 50%
  - More efficient than two previous attack schemes
  - Convenient for fault with distinctive pattern or low repeatability
Simplification of an existing DFA

- Only one column correspond to the right key hypothesis
- Visual discrimination between right and false hypothesis
- Easy to identify pattern from random value
- Only 3.5 faulted text with repeatability of 50%
- More efficient than two previous attack schemes
- Convenient for fault with distinctive pattern or low repeatability

DFA Results

<table>
<thead>
<tr>
<th>Realization</th>
<th>K10 hypothesis k</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0x00, 0x01, ..., 0xCD, ..., 0xFF</td>
</tr>
<tr>
<td>1</td>
<td>0x63, 0x61, ..., 0x02, ..., 0x15</td>
</tr>
<tr>
<td>2</td>
<td>0xB2, 0x0A, ..., 0x06, ..., 0x59</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>158</td>
<td>0x51, 0xFF, ..., 0x06, ..., 0x1A</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>3,578</td>
<td>0xF2, 0x49, ..., 0x08, ..., 0x82</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>10,000</td>
<td>0x09, 0x3B, ..., 0x0A, ..., 0x33</td>
</tr>
</tbody>
</table>
Fault injection

- With large spot size (125µmx125µm)
  - Bit-flip fault model observed
  - Bit set/reset observed too
    - Unexpected
  - Metal fills act as shutter on the laser beam
- Single-bit injected thanks to the metal coverage
- Laser injection
  - Data dependent
  - Time dependent
Exploitation of the data with DFA

- **Efficiency with high repeatability**
  - Giraud and Roche‘s DFA are not the most efficient

- Simple application of a DFA proposed
  - More efficient with low repeatability
  - Exploit fault injection pattern
Thank you for your attention

Questions?