Optical Fault Masking Attacks

Sergei Skorobogatov

http://www.cl.cam.ac.uk/~sps32  email: sps32@cam.ac.uk
Introduction

• Memory modification attacks were actively used in mid 90s to circumvent the security in microcontrollers
• In old chips a high voltage was supplied to an external pin to drive the memory control and programming circuit
• Modern chips have internal charge pumps and this prevents low-cost non-invasive attacks on memory
• Semi-invasive attacks in the form of optical fault injection were introduced at CHES-2002 and they use low-cost approach when a chip is attacked without establishing any physical contact to its internal components
• The presented research shows how embedded memory write and erase operations can be disabled using semi-invasive attacks thus raising security concerns
Background

• Flash memory structure
  – high voltages required for operation
  – narrow data bus
  – dedicated control logic

Diagram of flash memory structure with high voltage charge pumps, Y decoder, flash memory cells, X decoder, latches, and read sense amplifiers.
Experimental setup

• Sample preparation for PIC16F84, 16F628 and 16F628A
  – straightforward operation using simple chemistry lab
Experimental setup

- Test board for memory access via ICSP interface
- The chip was placed in a test socket mounted on XYZ-stage under a microscope with 20× objective lens
- Red laser diode module was used, 650nm, 25mW power
Results

• Locating Flash and EEPROM in PIC16F84 (1.2µm)
  – high-density areas with regular structure
  – the memory control is nearby
Results

• Locating Flash and EEPROM in PIC16F628 (0.9 µm)
  – high-density areas with regular structure
  – the memory control is nearby
Results

• Locating Flash and EEPROM in PIC16F628A (0.5μm)
  – high-density areas with regular structure
  – the memory control is nearby
Results

• Influence on memory Write and Erase operations
  – 10mW 650nm laser with front-side approach
  – tables show number of Cells/Lines protected at a time

• Whole memory disable with timing control delivers the perfect write protection tool

<table>
<thead>
<tr>
<th>Chip</th>
<th>Flash Cells</th>
<th>Flash Lines</th>
<th>Flash Array</th>
<th>EEPROM Cell</th>
<th>EEPROM Lines</th>
<th>EEPROM Array</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIC16F84</td>
<td>4 – 19</td>
<td>1 – 2</td>
<td>Yes</td>
<td>2 – 6</td>
<td>1 – 2</td>
<td>Yes</td>
</tr>
<tr>
<td>PIC16F628</td>
<td>2 – 16</td>
<td>1 – 2</td>
<td>Yes</td>
<td>2 – 4</td>
<td>1 – 2</td>
<td>Yes</td>
</tr>
<tr>
<td>PIC16F628A</td>
<td>1 – 2</td>
<td>1 – 2</td>
<td>Yes</td>
<td>1 – 2</td>
<td>1 – 2</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chip</th>
<th>Flash Cells</th>
<th>Flash Lines</th>
<th>Flash Array</th>
<th>EEPROM Cell</th>
<th>EEPROM Lines</th>
<th>EEPROM Array</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIC16F84</td>
<td>4 – 16</td>
<td>1 – 2</td>
<td>Yes</td>
<td>1 – 4</td>
<td>1 – 2</td>
<td>Yes</td>
</tr>
<tr>
<td>PIC16F628</td>
<td>2 – 13</td>
<td>1 – 2</td>
<td>Yes</td>
<td>2 – 3</td>
<td>1 – 2</td>
<td>Yes</td>
</tr>
<tr>
<td>PIC16F628A</td>
<td>No</td>
<td>1 – 2</td>
<td>Yes</td>
<td>No</td>
<td>1 – 2</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Experimental setup

• Backside sample preparation for PIC16F628A (0.5µm)
  – no chemicals involved
  – very simple, quick and easy operation
Results

• Microscope setup with a test socket and 20× objective lens
• Infrared laser diode module was used, 1065nm, 75mW
• Locating Flash and EEPROM in PIC16F628A (0.5µm)
  – position is known from the front-side experiments
  – the memory control is nearby
Results

• Influence on memory Write and Erase operations
  – 25mW 1065nm laser with backside approach
  – tables show number of Cells/Lines protected at a time

<table>
<thead>
<tr>
<th>Chip</th>
<th>Flash Cells</th>
<th>Flash Lines</th>
<th>Flash Array</th>
<th>EEPROM Cell</th>
<th>EEPROM Lines</th>
<th>EEPROM Array</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIC16F628A</td>
<td>1 – 2</td>
<td>1 – 2</td>
<td>Yes</td>
<td>1 – 2</td>
<td>1 – 2</td>
<td>Yes</td>
</tr>
<tr>
<td>PIC16F628A (backside)</td>
<td>12 – 45</td>
<td>1 – 2</td>
<td>Yes</td>
<td>8 – 22</td>
<td>1 – 2</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chip</th>
<th>Flash Cells</th>
<th>Flash Lines</th>
<th>Flash Array</th>
<th>EEPROM Cell</th>
<th>EEPROM Lines</th>
<th>EEPROM Array</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIC16F628A</td>
<td>No</td>
<td>1 – 2</td>
<td>Yes</td>
<td>No</td>
<td>1 – 2</td>
<td>Yes</td>
</tr>
<tr>
<td>PIC16F628A (backside)</td>
<td>10 – 36</td>
<td>1 – 2</td>
<td>Yes</td>
<td>10 – 27</td>
<td>1 – 2</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Experimental setup

• Backside sample preparation for MSP430F112 (0.35µm)
  – no chemicals involved
  – very simple, quick and easy operation

• Microscope setup with a test socket and 20× objective lens
Results

- Infrared laser diode module was used, 1065nm, 75mW
- Locating Flash in MSP430F112 (0.35 µm)
  - high-density areas with regular structure and large control
  - the memory control is nearby
Results

• Influence on memory Write and Erase operations
  – 25mW 1065nm laser with backside approach for PIC16F628A
  – 75mW 1065nm laser with backside approach for MSP430F112
  – power supply of MSP430F112 chip was reduced to 2.5V
  – tables show number of Cells/Lines protected at a time

<table>
<thead>
<tr>
<th>Chip</th>
<th>Flash Cells</th>
<th>Flash Lines</th>
<th>Flash Array</th>
<th>EEPROM Cell</th>
<th>EEPROM Lines</th>
<th>EEPROM Array</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIC16F628A (backside)</td>
<td>12 – 45</td>
<td>1 – 2</td>
<td>Yes</td>
<td>8 – 22</td>
<td>1 – 2</td>
<td>Yes</td>
</tr>
<tr>
<td>MSP430F112 (backside)</td>
<td>28 – 60</td>
<td>1 – 2</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chip</th>
<th>Flash Cells</th>
<th>Flash Lines</th>
<th>Flash Array</th>
<th>EEPROM Cell</th>
<th>EEPROM Lines</th>
<th>EEPROM Array</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIC16F628A (backside)</td>
<td>10 – 36</td>
<td>1 – 2</td>
<td>Yes</td>
<td>10 – 27</td>
<td>1 – 2</td>
<td>Yes</td>
</tr>
<tr>
<td>MSP430F112 (backside)</td>
<td>19 – 40</td>
<td>1 – 2</td>
<td>Yes (unstable)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Limitations and improvements

• Fault masking attacks
  – work for other embedded memory, e.g. SRAM (S. Skorobogatov: Optically Enhanced Position-Locked Power Analysis, CHES-2006)
  – not very effective for single-cell influence
  – works well for disabling bit-lines, word-lines and a whole chip

• Modern chips with three or more metal layers
  – backside approach is the only solution as the optical path is blocked

• Backside approach
  – higher laser power is required for reliable influence
  – lower spatial resolution, hence, better optics is required

• Power supply voltage influence on PIC16F628 chip

<table>
<thead>
<tr>
<th>PIC 16F628</th>
<th>2.5 V</th>
<th>3.0 V</th>
<th>3.5 V</th>
<th>4.0 V</th>
<th>4.5 V</th>
<th>5.0 V</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laser power, mW</td>
<td>2.4</td>
<td>4.6</td>
<td>6.1</td>
<td>7.2</td>
<td>7.9</td>
<td>8.5</td>
</tr>
</tbody>
</table>
Countermeasures

• Use of modern chips with multiple metal layers forces an attacker to use backside approach and results in more expensive and longer attack

• Metal shielding over sensitive areas can help but cannot prevent backside approach

• Light sensors could detect the attack but will require more sophisticated hardware

• Encryption, redundancy check and address permutations make analysis harder, but cannot eliminate it completely

• Data verification after writing can help, however, the read operation can be influenced as well by using fault injection
Conclusions

• Optical fault masking attacks can be applied using semi-invasive techniques without sophisticated chip preparation techniques
• Optical fault masking attacks offer possibility of partial reverse engineering for chips by finding active locations
• Backside approach helps in modern chips and it is easy to perform
• At a lower power supply voltage less power of laser is required for the attack
• Lack of protection against optical fault masking attacks in modern chips might lead to possible vulnerabilities