Using Optical Emission Analysis for Estimating Contribution to Power Analysis

Dr Sergei Skorobogatov

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

• Power analysis attacks were introduced in 1999 (Kocher et al), and exploit well known fact that power consumption of a chip is correlated with its operation and processed data.

• Semi-invasive attacks in a form of optical fault injection were introduced in 2002 (Skorobogatov et al), and use low-cost approach when a chip is attacked without establishing any physical contact to its internal components.

• Optical emission analysis attacks were introduced in 2008 (Ferrigno et al), and exploit well known fact that photon emission of a chip is correlated with processed data.

• The presented research shows how optical emission analysis attacks can be done at a low cost and how they can be used to improve protection against power analysis.
Background

• Optical emission from CMOS circuits
  – known for over 40 years
  – actively used in failure analysis for over 20 years

• Can be used to compromise security in silicon chips
  – so far required expensive equipment and special chip preparation
  – was not considered as a threat, hence, no protection is in place
Background

• Number of photons emitted per every switch

\[ N_e = S_e B \left( \frac{L_H I_d}{qv_s} \right) T_s \sim 10^{-2} \ldots 10^{-4} \text{ ph/switch} \]

\( S_e \) – spectral emission density, \( B \) – emission bandwidth,
\( L_H \) – hot-carrier region length, \( I_d \) – drain current, \( q \) – e\(^{-}\) charge,
\( v_s \) – carrier saturated velocity, \( T_s \) – transition time

• Only 5~10\% of photons can reach the sensor (direction and losses)

• Existing analysis techniques
  – picosecond imaging circuit analysis (PICA) uses photomultiplier arrays
  – photon emission microscopy (PEM) uses special IR cameras

• Correlation between photon emission and power consumption
Experimental setup

- Sample preparation (PIC16F628)
- Locating Flash, EEPROM, SRAM, CPU
- Choosing PMT, APD and CCD sensors
Experimental setup

- Choosing PMT: low dark current
- Choosing APD: high quantum efficiency
- Choosing CCD: NIR sensitivity, low dark current

<table>
<thead>
<tr>
<th>Type of camera</th>
<th>Wave-length, nm</th>
<th>QE at 900 nm</th>
<th>QE at 1000 nm</th>
<th>Dark current e$^-$/s</th>
<th>Time response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantar Mepsicron II S25</td>
<td>180–940</td>
<td>1%</td>
<td>0%</td>
<td>0.005</td>
<td>50 ps</td>
</tr>
<tr>
<td>Hamamatsu C4880-21</td>
<td>200–1200</td>
<td>50%</td>
<td>20%</td>
<td>0.3</td>
<td>20 ms</td>
</tr>
<tr>
<td>Hamamatsu C4880-50</td>
<td>200–1100</td>
<td>30%</td>
<td>10%</td>
<td>0.01</td>
<td>20 ms</td>
</tr>
<tr>
<td>Hamamatsu H10330-25</td>
<td>850–1250</td>
<td>2%</td>
<td>2%</td>
<td>2000</td>
<td>900 ps</td>
</tr>
<tr>
<td>Hamamatsu H6780-01</td>
<td>250–850</td>
<td>&lt;1%</td>
<td>0%</td>
<td>400</td>
<td>780 ps</td>
</tr>
<tr>
<td>Sensl PCDMini-0020</td>
<td>400–1100</td>
<td>2%</td>
<td>&lt;1%</td>
<td>50</td>
<td>200 ps</td>
</tr>
<tr>
<td>Sony Super HAD CCD</td>
<td>300–1050</td>
<td>8%</td>
<td>1%</td>
<td>0.02</td>
<td>10 μs</td>
</tr>
<tr>
<td>Sony EXview HAD CCD</td>
<td>300–1100</td>
<td>12%</td>
<td>5%</td>
<td>0.02</td>
<td>10 μs</td>
</tr>
</tbody>
</table>
Experimental setup

- PMT setup: decapsulated chip facing sensor's aperture
- CCD setup: camera mounted on a microscope, chip placed in a test socket
- Hamamatsu H6780-01 PMT sensor
- Starlight Xpress SXV-H9 CCD camera
Results

- PIC16F628 was running at 20MHz clock (5 MIPS) with 6V power supply
  - PMT: H6780-01, 60' acquisition
  - SPA: 10Ω resistor, active probe

- PMT vs SPA
  - higher bandwidth
  - possible localisation
  - special hardware will suit better as oscilloscope is not designed for integration

- Test code: `bsf portb,3`  
  `clrf 0x75`  
  `decf 0x75,f`  
  `bcf portb,3`  
  `goto loop`
Results

• CCD
  – 2x objective lens
  – 30' integration time
  – continuous read of EEPROM and SRAM:
    incf EEADR,f
    bsf EECON1,RD
    movf EEDATA,w
    decf 0x75,f
    goto loop
Results

- EEPROM
  - 10x objective lens
  - 10' integration time
  - read 4 addresses in a loop
  - data: 56h, 56h, 56h, 00h

- Flash memory has similar structure and gives similar results
Results

- **SRAM**
  - 10x objective lens
  - 10' integration time
  - read A6h: movf 0x75,w
  - write W=A6h: movwf 0x75
  - XOR W=C3h, (0x74)=A6h, xorwf 0x74,f
Limitations and improvements

- Data recovery
  - slow process: minimum 1 minute per byte

- Modern chips
  - three or more metal layers prevent direct observation and analysis
  - smaller technologies require longer integration time

- Backside approach
  - silicon is transparent to light wavelengths above 1000 nm
  - lower spatial resolution
  - longer integration time due to higher losses in silicon and optics
  - higher magnification lenses give better result
  - use of NIR optics improves result (expensive)
  - substrate thinning might be useful for faster analysis (expensive)
  - increase of the power supply voltage boosts the optical emission
Limitations and improvements

- Increasing the power supply voltage: every 10% increase boosts the emission by 40~120%

<table>
<thead>
<tr>
<th>Power Supply Voltage</th>
<th>PIC16F628</th>
<th>130nm ASIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5 V</td>
<td>1046</td>
<td>889</td>
</tr>
<tr>
<td>4.0 V</td>
<td>1286</td>
<td>1194</td>
</tr>
<tr>
<td>4.5 V</td>
<td>2427</td>
<td>1953</td>
</tr>
<tr>
<td>5.0 V</td>
<td>8400</td>
<td>5270</td>
</tr>
<tr>
<td>5.5 V</td>
<td>23292</td>
<td>9536</td>
</tr>
<tr>
<td>6.0 V</td>
<td>43026</td>
<td>23270</td>
</tr>
</tbody>
</table>
Limitations and improvements

• 16F628 vs 16F628A: 0.9 µm and 0.5 µm, higher density with CMP technology leads to ~80% loss in intensity
Limitations and improvements

• PIC16F628: EEPROM area from front and rear sides after 30' of integration with standard 10x objective lens
Limitations and improvements

• Backside approach
  – 0.13 µm ASIC with SRAM
  – Vcc increased from 1.5 V to 2.0 V (6x boost of emission)
  – 20x NIR objective
  – 60' integration time
Countermeasures

• Use of modern chips with multiple metal layers forces an attacker to use backside approach and results in longer time required for the attack
• Metal shielding over sensitive areas can help but cannot prevent backside analysis
• Encryption and redundancy check make analysis harder
• Asynchronous circuits could make the attack more problematic as data analysis requires a single byte to be present at a specific time
Conclusions

• Optical emission analysis can be carried out at a relatively low cost using hobbyist astronomical CCD cameras
• PMT offers high bandwidth and acquired data have correlation with power analysis results
• Results of optical emission analysis can be used for finding weak spots in protection against power analysis attacks
• Optical emission analysis offers possibility for partial reverse engineering of chips including data analysis
• Backside approach can help in modern chips, but has lower spatial resolution and requires longer integration time
• Increase of the power supply voltage boosts the optical emission and considerably reduces time of analysis
• Lack of protection against optical side-channel attacks in modern chips might lead to possible vulnerabilities