On the Complexity Reduction of Laser Fault Injection Campaigns using OBIC Measurements

Falk Schellenberg, Markus Finkeldey, Bastian Richter, Maximilian Schäpers, Nils Gerhardt, Martin Hofmann and Christof Paar
Motivation

Fault injection into integrated circuits
  - Clock glitches
  - Voltage alterations
  - EM
  - Light (UV, flash lamps, laser)

Parameters for successful fault injection
  - Timing (clock cycle and time within clock cycle)
  - Length
  - Physical intensity

Additional parameters for laser fault injection
  - Focus (/spot size) (z)
  - Location (x/y)
  - Doubled for two-spot systems

→ Large search space, exhaustive search might be infeasible
Reducing Search Space (1)

Carpi et al.: “Glitch It If You Can: Parameter Search Strategies for Successful Fault Injection”, CARDIS13
Picek et al.: “Evolving genetic algorithms for fault injection attacks”, MIPRO14
Picek et al.: “Fault Injection with a new Flavor: Memetic Algorithms make a difference”, COSADE15 (*)

Idea: Use machine learning for finding parameters

Hardly applicable to all parameters (timing, laser location)
Reducing Search Space (2)

Franck Courbon et al.: “Increasing the efficiency of laser fault injections using fast gate level reverse engineering”, HOST14

Idea:
1. Grind/polish down to doped area
2. Capture SEM images, identify **flip-flops**, find all other instances by correlation
3. Use locations for laser fault injection

Requires access to SEM, profiling sample gets destroyed
Importance of Flip-Flops

Fault has to be stored by a register, otherwise no effect

By directly targeting flip-flops
- Every possible single bit fault
- However, no multi bit faults
Optical Beam Induced Current

In a nutshell:
Use DUT as “really bad” photodiode → Measure current created at pn-junctions
Our Proposal

Optical Beam Induced Current (OBIC) as imaging technique
- High resolution
- Identify locations (x,y,z)
- Find flip-flops
→ Reduces number of Points of Interest drastically

Advantages:
- Independent of other parameters (e.g., power, delay, length)
- Chip is not powered → no countermeasures can be active
- Minimal equipment overhead
- Possible with “every” laser setup

Disadvantage:
- Resolution not as powerful as SEM etc.
OBIC in Literature

- Well-known in (production-) fault analysis
- Security context:

(a) Unknown chip, backside!
(b) Motorola µC, SRAM, frontside
(c) Microchip µC, 0.9µm, SRAM, frontside
(d) NEC µC, 0.35µm, backside
   Actel FPGA, 0.13µm, backside

Image Sources:
(a) van Woudenberg et al., Practical optical fault injection on secure microcontrollers, FDTC11
(b) Skorobogatov, Semi-invasive attacks - A new approach to hardware security analysis, 2005
(c) Skorobogatov, Optically enhanced position-locked power analysis, CHES06
(d) Skorobogatov, Flash memory ‘bumping’ attacks, CHES 2010
Setup

Measurement

Self-build setup
- Lumics laser diode at 1064nm, SMF
- Leica NIR objective (NA 0.75, 100x)
- Newport XPS with motorized stages
- FEMTO transimpedance amplifier connected to VDD/GND
- Stanford Research low noise amplifier

Fault Injection

Modified commercially available LFI setup
- Alphanov PDM 975nm 2W diode, SMF
- Mitutoyo Plan Apo NIR HR (NA 0.65, 50x)
- Märzhäuser and PI stages

Image Source: alphanov.com
Case Study: ATX Mega16A4U

ATX Mega16A4U, 250nm

– Hardware Encryption
  • DES (“Round”-Instruction)
  • AES (Start/End-Flags)

– Backside thinned to approx. 20µm
Case Study: ATXMEga16A4U

(1) Rough estimation by EM analysis (optional)
- Self-made probe with amplifier
- Trigger during encryption → clearly visible peaks
Case Study: ATX Mega 16A4U

(2) OBIC Measurement around found area (z)

- Find focal plane resulting in maximum current
- \( \rightarrow \) Optimal z-Position for OBIC and LFI
- Enables to account for tilted DUT with very high precision
Case Study: ATX Mega16A4U

(2) OBIC Measurement around found area (x/y)
Case Study: ATX Mega16A4U

(3) Correlation-Based Pattern Recognition

Pearson correlation 0.6 up to ~0.8

Four times for each orientation

In a matter of seconds
Case Study: ATX Mega16A4U

(3) Correlation-Based Pattern Recognition

Colors consistent
Case Study: ATXMega16A4U

(4) Correct Timing (SHORTCUT)

- Know-key correlation on intermediate values
- Example: Hamming Distance of state bytes $s_i$

$$HD(s_i, s_{i+1})$$ at input of last round
Case Study: ATX Mega 16A4U

(5) Laser Fault Injection
Case Study: ATX Mega16A4U

(5) Laser Fault Injection - Detail

Calculated backwards based on known key
Green: Bit Set
Red: Bit Reset

(a) Complementary fault pattern consistent
    → Storage part?

(b) Changing third sensitivity zone
    → Clock input?
    → Reset?

Pattern identical when clock halted during LFI
    → Confirms flip-flop identification
(6) Differential Fault Analysis

Straightforward approach worked quite well:

1. Fault between MixColumns (9th round) and SubBytes (10th round) $\rightarrow$ single byte faults at output

2. Test for which key hypothesis the difference between faulty ciphertext and genuine ciphertext byte resolves to single bit fault before SBox

$\rightarrow$ approx. two pairs ciphertext/faultytext per byte
Discussion (1)

Time Improvement

- Required time linearly depends on positions to test
- At 1µm steps for given area and 34 found flip-flops:
  - 255 * 150 = 38250 points exhaustive search
  - 34 * 17 * 10 = 5780 only flip-flop area
- Targeting only sensitive areas: 3 * 34 = 102
Applicability

Influencing parameters

- Technology node (ATXmega16A4U: 250nm)
- Characteristic cell layout (ATXmega16A4U: 17µm*10µm area)
- Effective spot size (our setup: approx. 710nm calculated spatial resolution)

→ ATXmega16A4U: plenty of structural detail for given resolution

Smaller technology nodes:

- Averaging, fine-adjusting laser energy, 2-photon absorption, solid immersion lenses
- Potentially hard to manually identify flip-flops
- Autocorrelation?
- Future work..
Conclusion

- Used OBIC measurement as profiling to find flip-flops
  - Device shut off (no reactive countermeasures)
  - Independent of correct timing, pulse length (, energy)
- Reduced search space by factor of 6.6 or 375
- Successfully attacked ATX Mega 16A4U AES core

Countermeasures:
- Isolated power supply (probe bulk directly?)
Thanks!
Questions?