Low-cost Setup for Localized Semi-invasive Optical Fault Injection Attacks

Oscar M. Guillen[1]   Michael Gruber[2]   Fabrizio De Santis[2]

[1] Giesecke & Devrient
[2] Technische Universität München

COSADE 2017

Table of contents

Motivation

- Fault Injection in practice:
  - Are local optical attacks feasible using low cost equipment ($\sim$ €500)?
  - What kind of faults can be generated?

Motivation

The cost of the equipment is important for security evaluation

- Attack rating
  - Equipment
  - Level of expertise
- Low-cost devices
  - Microcontroller-based devices
  - IoT endpoints

Fault Injection Techniques

Technique	Accuracy (Spatial)	Accuracy (Temporal)	Cost	Risk (Damage)
Clock glitch	none	high	low	none
Voltage spike	none	high	low	low
Heat	low	none	low	low
EM Pulse	medium	medium	medium	medium
Laser beam	high	high	high	medium

Table : Summary of non-invasive fault injection techniques [1]

Optical Fault Injection

Complete fault injection stations cost up to €150k [3]

- Light source
  - Flashgun, for older technology nodes [6]
  - Laser, newer technologies
- Focusing element
  - Visible-light microscope
  - Infrared microscope and camera
- Positioning
  - X-Y Stage

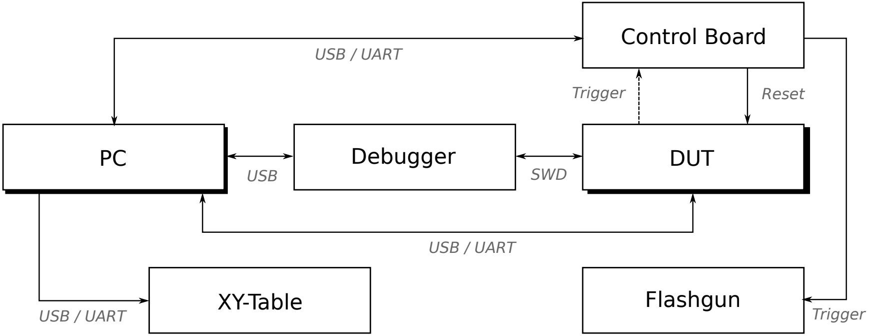
Low-cost Optical Fault Injection

Our low-cost fault injection setup $\sim$ €500

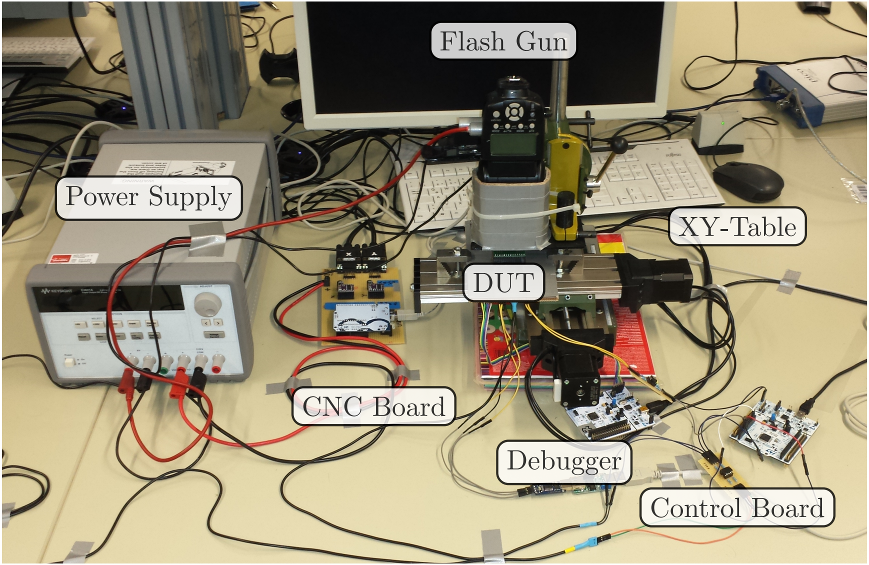
- Light source
  - Flashgun
- Focusing element
  - Ball lens 'microscope'
- Positioning
  - X-Y Micro-milling stage (5 µm resolution)
  - Motor control using grbl [5]
  - Z-axis operated manually
- DUT's minimal setup boards
  - AVR 8-bit,
    Atmega328p, 350 nm
  - ARM Cortex M0 32-bit,
    STM32F030F4P6, 90 nm

Table of contents

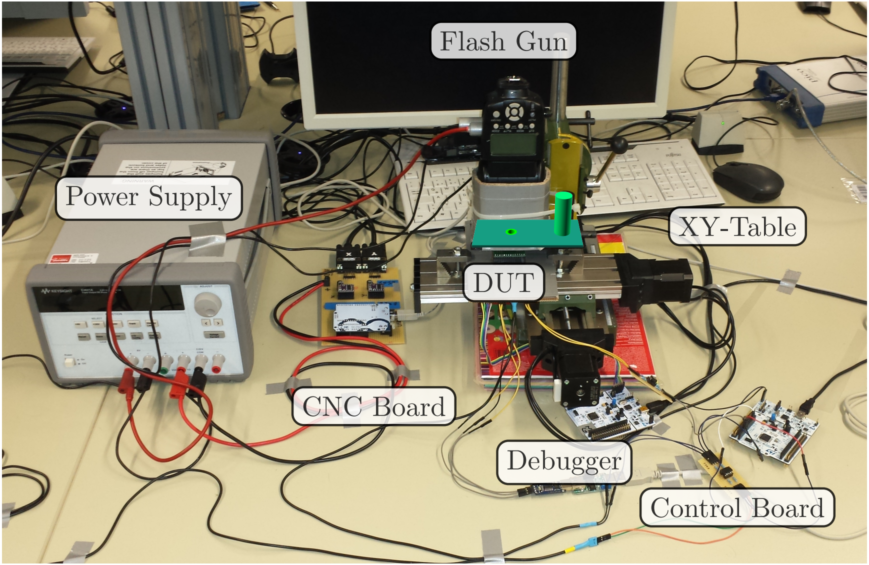
Block Diagram



Fault Injection Setup



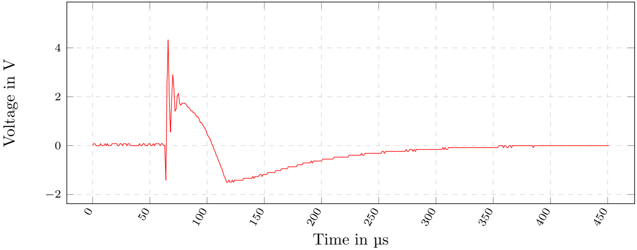
Fault Injection Setup



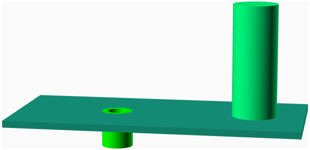
Fault Injection Setup

Light source

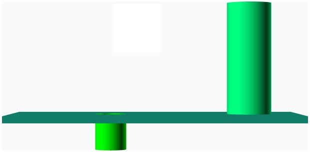
- Flashgun
- Trigger Delay of 64 µs
  (measured using a LED to sense emitted light)



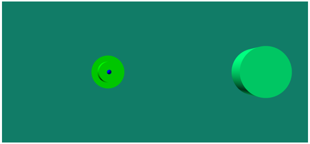
3D Printed Mount for the Optics



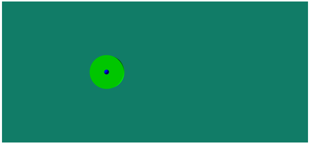
(a) Side I



(b) Side II



(c) Top



(d) Bottom

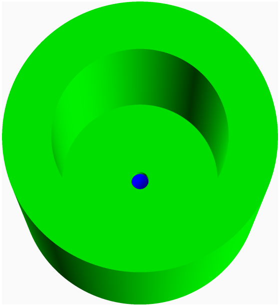
Optics

- Ball Lens
- Diameter 1 mm
- Substrate N-BK7
- Wavelength 350 nm to 2200 nm
- Diameter Tolerance ±2.5 μm
- Back Focal Length (BFL) 0.23 mm
- Mounted in 3d printed socket

Front-View

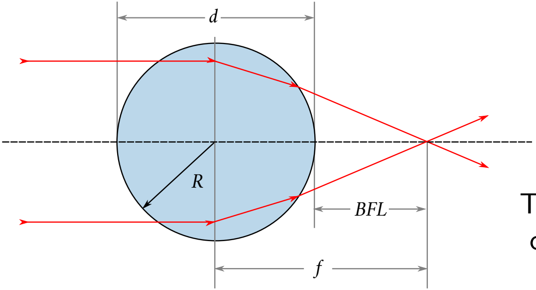
Optics

- Ball Lens
- Diameter 1 mm
- Substrate N-BK7
- Wavelength 350 nm to 2200 nm
- Diameter Tolerance ±2.5 µm
- Back Focal Length (BFL) 0.23 mm
- Mounted in 3d printed socket



Top-View

Ball lens



Ball lens focal point,

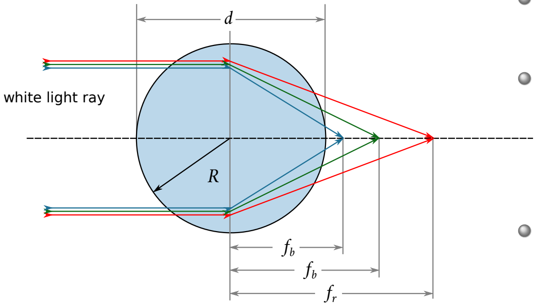
$$\frac{1}{f} = \frac{4(n-1)}{n \cdot d} \qquad (1)$$

The magnification M of a lens compared to a human eye is:

$$M = \frac{250\,\text{mm}}{f} \qquad (2)$$

for a 1.0 mm diameter, N-BK7 borosilicate-glass ball lens $n = 1.517$
$f = 0.733\,56\,\text{mm}$, $BFL = 0.233\,56\,\text{mm}$, $M = 340\times$

Ball lens



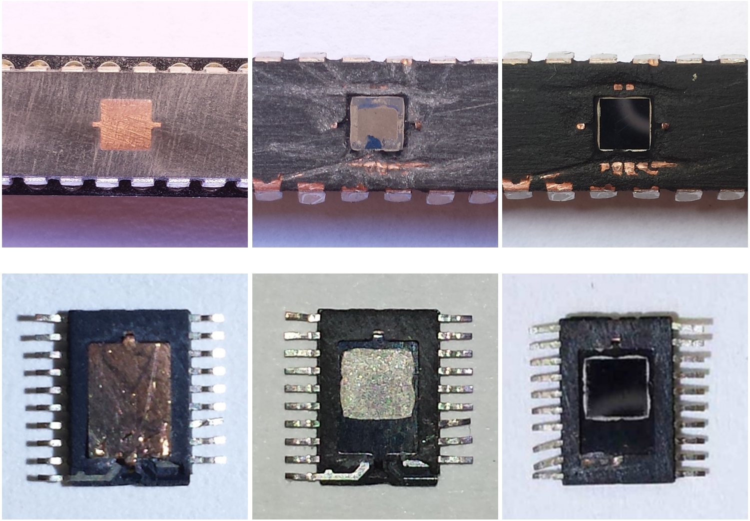
- White light is composed of different wavelengths
- Light components are dispersed according to their frequency (chromatic aberration)
- Infrared component (wavelength $>$715 nm) is present in the light generated by the flashgun and focused through the ball lens

Preparation I

- Semi-invasive attacks require a decapsulated DUT
  - Frontside: dangerous, using chemicals
  - Backside: easy, but no visible structures
- Decapsulation procedure:
  1. Grind down the backside using sandpaper
  2. Pry the lead frame open using a knife
  3. Clean the chip from glue using acetone

	ARM Cortex M0	AVR
Package	TSSOP	PDIP
Grinding	−	−
Opening	−	+
Cleaning	−	+

Preparation II



(a) Sanding (b) Removing (c) Cleaning

Fault Characterization I

- Instruction Skip Test (global/local)
  1. Execute function
  2. Inject fault
  3. Check result
- RAM Faults (global/local)
  1. Write pattern to RAM
  2. Inject fault
  3. Check result
- Register Faults (local)
  1. Pre-set user accessible registers
  2. Inject fault
  3. Read back registers
- Procedure:
  1. Generate meander pattern
  2. Perform test
  3. Read result
  4. Update position
  5. `goto #2`

Fault Characterization II

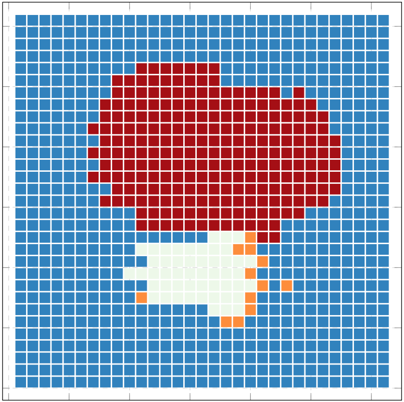
Fault Injection Results

	Atmega328p (350 nm)		STM32F030F4P6 (90 nm)	
	local	global	local	global
Instruction Skip	✗	✓	✓	✗
Register Change	✗	✗	✓	✗
RAM Change	✓	✗	✗	✗

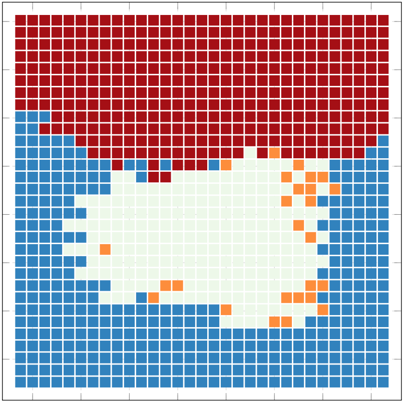
Fault Characterization III

ARM Cortex M0 32-bit, 90 nm, (STM32F030F4P6)

Reset, No change, Exploitable fault, Non-exploitable fault



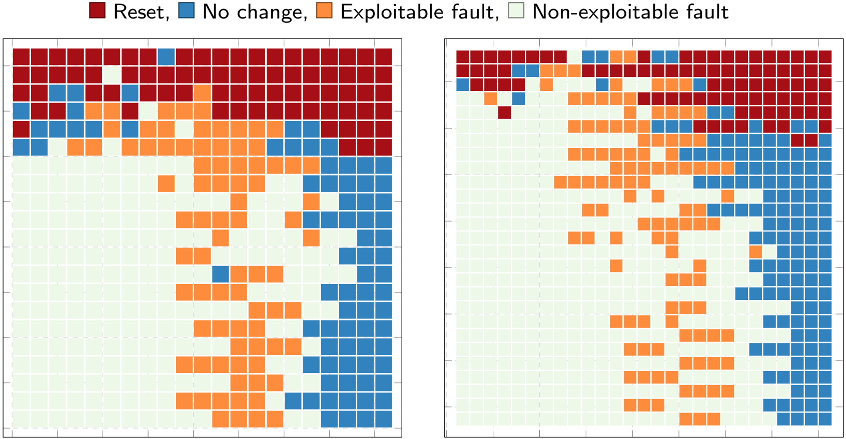
(a) Whole Chip, 0.1 mm, 3 mm × 3 mm



(b) ROI-1, 0.05 mm, 1.5 mm × 1.5 mm

Fault Characterization IV

ARM Cortex M0 32-bit, 90 nm, (STM32F030F4P6)



(c) ROI-2, 0.02 mm, 0.4 mm × 0.4 mm

(d) ROI-3, 0.015 mm, 0.4 mm × 0.4 mm

Table of contents

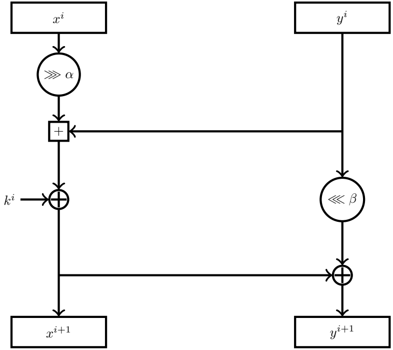
SIMON and SPECK

- Published by the NSA in 2013 [2]
- Lightweight block ciphers
- Perform well on resource constrained devices
- SIMON targets HW implementations
- SPECK targets SW implementations
- Each algorithm allows 10 different combinations of block/key size

block size	key size
32	64
48	72, 96
64	96, 128
96	96, 114
128	128, 192, 256

Details of SPECK

- Feistel-like structure
- ADD, ROT, XOR (ARX)
- T 22-34 rounds
- Break the 2,3,4 last rounds to recover key, depending on key size
- Key Schedule reuses the round function
- State y^{T-1} known



$$R(x, y) = (f(x, y) \oplus k, y \lll \beta \oplus f(x, y) \oplus k) \text{ where } f(x, y) = x \ggg \alpha + y$$

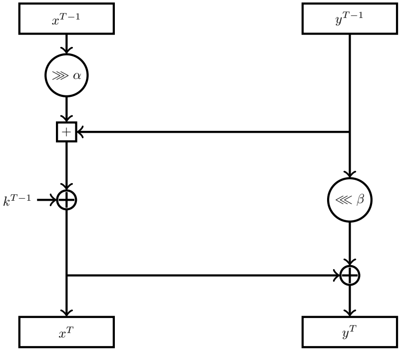
Application to SPECK I

- What kind faults can we generate?
- What kind of faults can we exploit?

Application to SPECK II

Instruction Skip

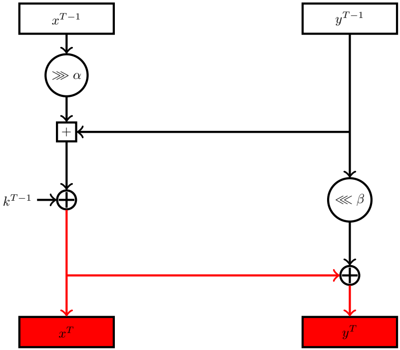
- AVR - *global setup*
- STM32 - *local setup*
- Skip XOR with k^{T-1}
- Less than 1 second
- Only 1 injection needed
- Recover k^{T-1} completely
- Same outcome in 80 % of the injections



Application to SPECK II

Instruction Skip

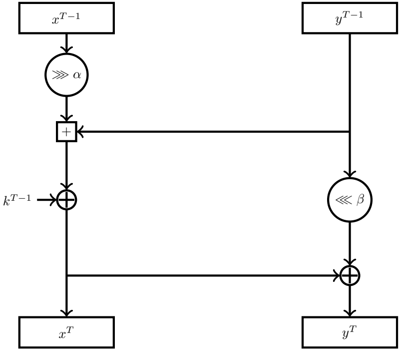
- AVR - *global setup*
- STM32 - *local setup*
- Skip XOR with k^{T-1}
- Less than 1 second
- Only 1 injection needed
- Recover k^{T-1} completely
- Same outcome in 80 % of the injections



Application to SPECK III

Random Fault/Register Fault [4]

- STM32 - *local setup*
- Random fault model at y^{T-1}
- Attack takes $\approx$1 h
- Attack needs $\approx 3 \times 10^3$ injections
- 46 faulty pairs recovered
- Recovers $n-1$ bits of k^{T-1} (MSB cannot be recovered due to the modular addition)



Application to SPECK III

Random Fault/Register Fault [4]

- STM32 - *local setup*
- Random fault model at y^{T-1}
- Attack takes ≈1 h
- Attack needs ≈3×10^3 injections
- 46 faulty pairs recovered
- Recovers $n-1$ bits of k^{T-1} (MSB cannot be recovered due to the modular addition)

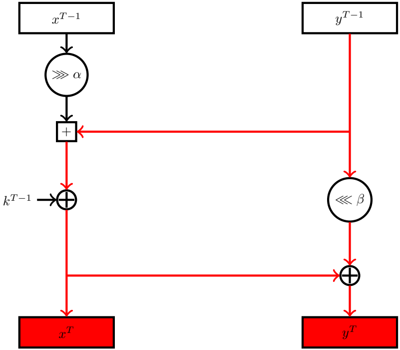


Table of contents

Summary

- Low cost localized fault injection setup
  - `https://github.com/open-fi/fault-injector`
- Backside fault injection
  - Cheap ball lens enables backside attacks with flashgun
  - Performed in unthinned devices
- Faults observed on 90 nm MCUs
  - Register manipulation
  - Instruction skip

Implications

- High security devices might already have countermeasures in place (e.g. optical sensors)
- Low-cost, microcontroller-based, devices should consider low-cost optical attacks as a serious threat

Future Work

- Different light sources
- Different types and sizes of focusing elements
- Pattern-based triggering
- EM Fault Injection

Costs

Function	Description	Price (EUR)
Optics		
Flashgun	YN560 III	60
Ball lens	1 mm N-BK7	25
Positioning		
X-Y Table	Proxxon KT 70	263
Stand	Proxxon Stand	70
Control	Arduino UNO	20
Drivers	DRV8825	18
Control and Debugging		
Control Board	STM32 Nucleo F411RE	12
Debugger	STM32 Nucleo F411RE (OpenOCD)	12
Miscellaneous		
	Sand paper, mask, latex gloves, acetone	26
		506

Thank you for your attention!

Bibliography

[1] Alessandro Barenghi, Luca Breveglieri, Israel Koren, and David Naccache. Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures. *Proceedings of the IEEE*, 100(11):3056–3076, 2012.

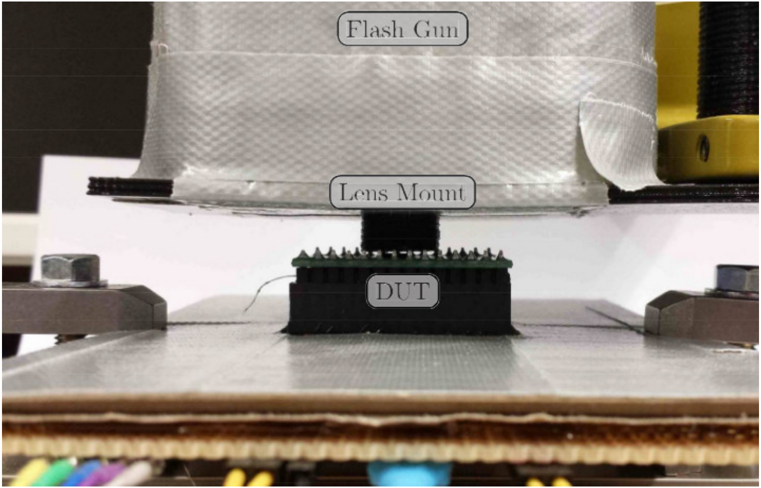
[2] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The simon and speck families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404, 2013. http://eprint.iacr.org/.

[3] Jakub Breier and Dirmanto Jap. Testing feasibility of back-side laser fault injection on a microcontroller. In *Proceedings of the WESS'15: Workshop on Embedded Systems Security*, WESS'15, pages 5:1–5:6, New York, NY, USA, 2015. ACM. ISBN 978-1-4503-3667-3. doi: 10.1145/2818362.2818367. URL http://doi.acm.org/10.1145/2818362.2818367.

[4] Yuming Huo, Fan Zhang, Xiutao Feng, and Li-Ping Wang. Improved differential fault attack on the block cipher speck. In *2015 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 28–34. IEEE, 2015.

[5] Sungeun K. Jeon, 2016. https://github.com/grbl/grbl.

[6] Sergei P. Skorobogatov and Ross J. Anderson. Optical fault induction attacks. In *Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers*, pages 2–12, 2002. doi: 10.1007/3-540-36400-5_2. URL http://dx.doi.org/10.1007/3-540-36400-5_2.


Flash Gun
Lens Mount
DUT