Switch-Glitch

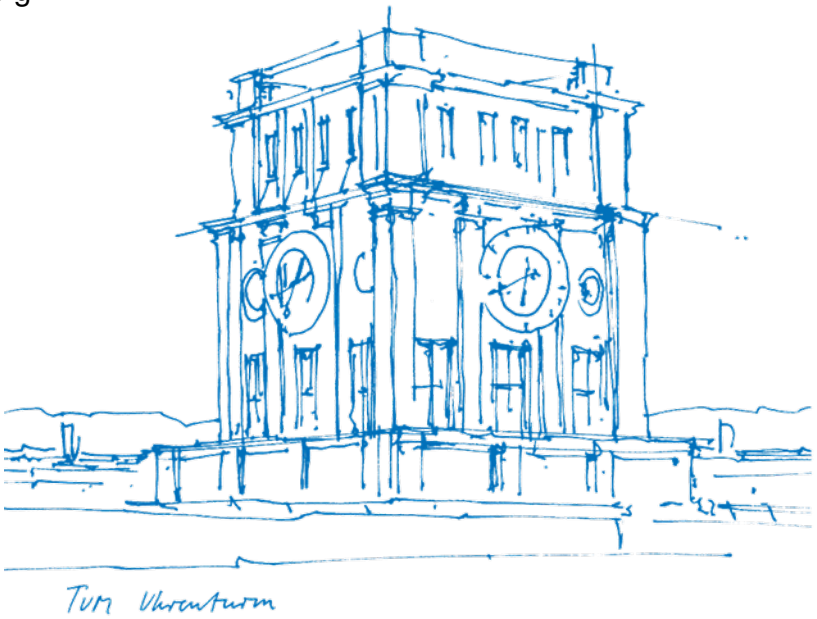
Location of Fault Injection Sweet Spots by Electro-Magnetic Emanation

Matthias Probst, Michael Gruber, Manuel Brosch, Tim Music, Georg Sigl

Technical University of Munich

TUM School of Computation, Information and Technology

Chair of Security in Information Technology



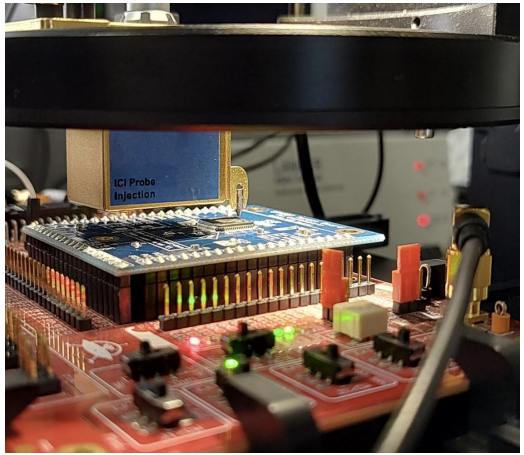
Overview

Introduction

Finding Position for EMFI means finding suitable parameters for

- x,y,z Position
- time t_{Fault}
- length Δt_{Glitch}
- strength V_{Fault}
- number of glitches
- ...

$\rightarrow$ This is takes a long time!
$\Rightarrow$ **We aim to speed up the process**



State-of-the-Art

Probe position for local Electro-Magnetic Emanation measurements:

- Statistical metrics find high SNR positions [6, 7]
- Leakage information to select positions [2, 8]
- machine learning [4]

EMFI local attacks focus on setups only:

- Breier and Jap use a laser for local fault injections [1]
- Guiellen et al. show low-cost setup to be effective for local fault injections [5]
- Ghodrati et al. inject local faults into a RISC-V core [3]

$\rightarrow$ EMFI position selection is not yet covered

$\Rightarrow$ Is there a relation between local EM positions and local EMFI positions?

$\Rightarrow$ Can we use this to our advantage?

Methodology

TVLA or SNR-test need

- multiple traces
- knowledge about processed data

EM hotspot identification with simple SNR

$$\mathrm{SNR} = \frac{\mu_T^2}{\sigma_T}$$

to collect as little data as possible.

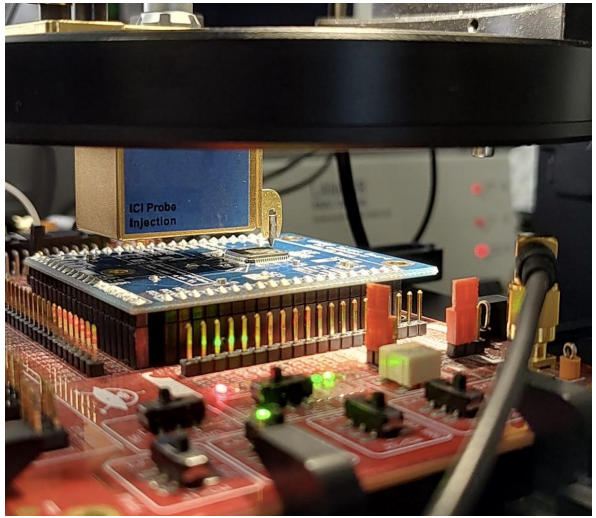
→ single trace T

→ no data-knowledge required

Testcode is used for both EMFI and SCA. For faults, we target second store of `r4` to `sp+12`.

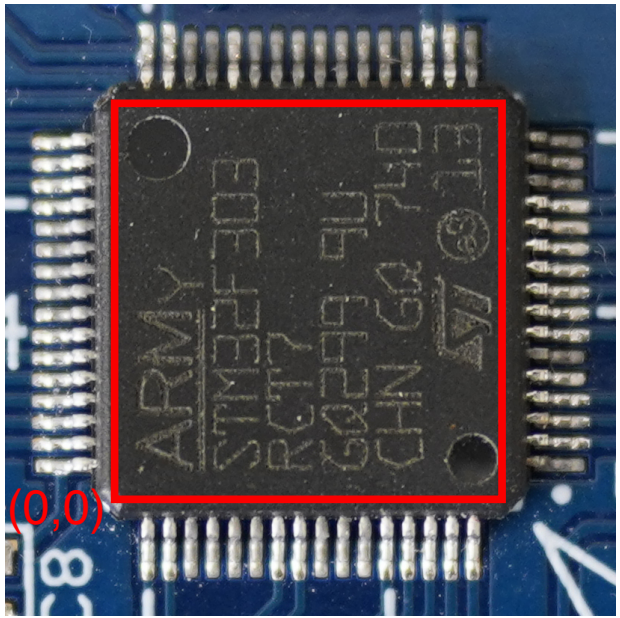
```
1   uint32_t inc, data[3] = {0,0,0};
2
3   set_trigger();
4   // function we want to glitch
5   asm("nop                         ;; 20 times
6        movs r4, #65 \n\t
7        strd r4, r4, [sp, #8]
8        nop                         ;; 20 times
9        str  r4, [sp, #16]");
10  reset_trigger();
11  send_data(data, sizeof(data));
```

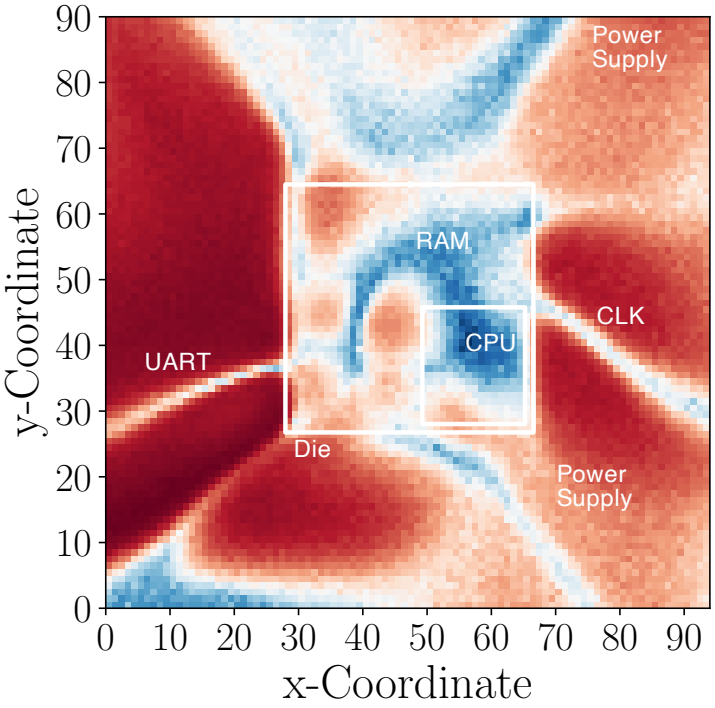
Experimental Setup



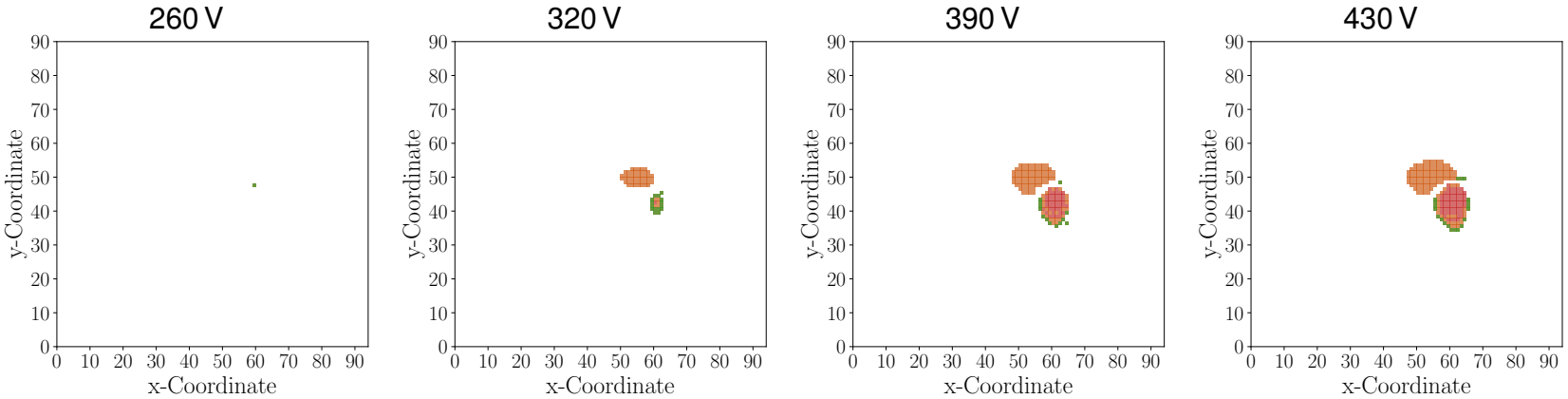
- **STM32F303** Microcontroller running at 48 MHz
- NewAE CW308 UFO Board as base PCB
- Picoscope 6402D (@ 2 GHz) with near-field EM probe with **resolution of 150 um** (Langer ICR HH250-75)
- Faults with **coil diameter of 500 um** (Langer BPS 202 and Langer ICI HH 500-15)
- **Power Cycle** during EMFI via FTDI UART bridge

Local EM emanations





Local Fault Injections I



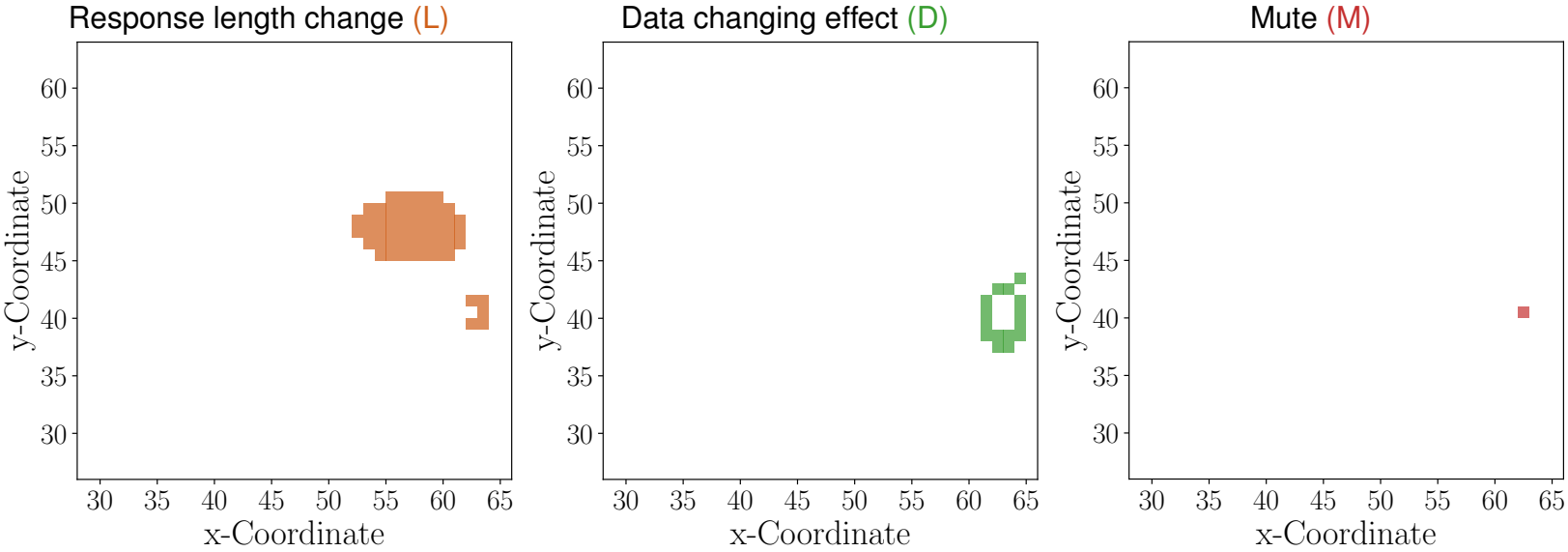
Fault parameters in addition to x- and y-direction:

- $\Delta t_{Fault} = 10\,\mu s$ (shortest possible)
- V_{Fault} from 150 V to 430 V in 10 V steps
- Offset from trigger is set to 50 ns

→ Lower voltage lead to (D) and (L) at about 320 V.

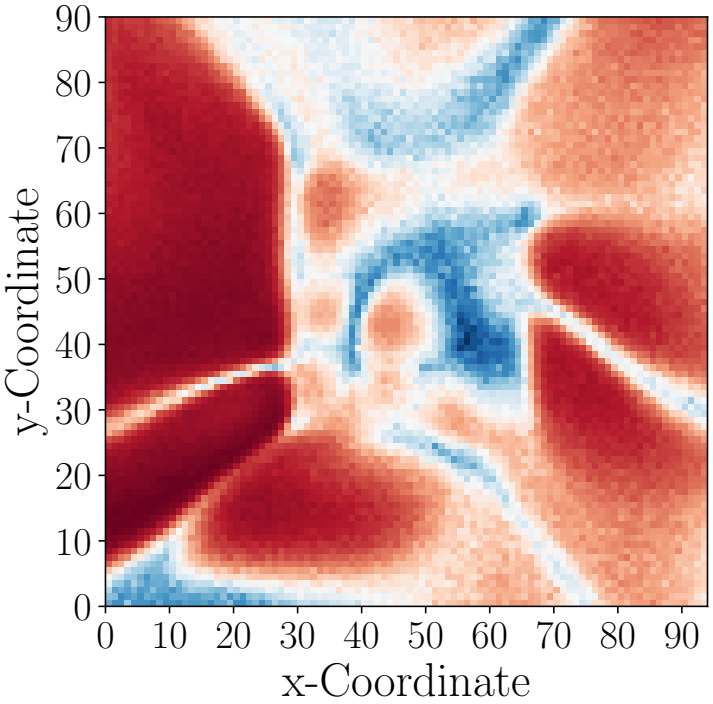
→ Increasing voltage further leads to increased (M) occurrences.

Local Fault Injections II



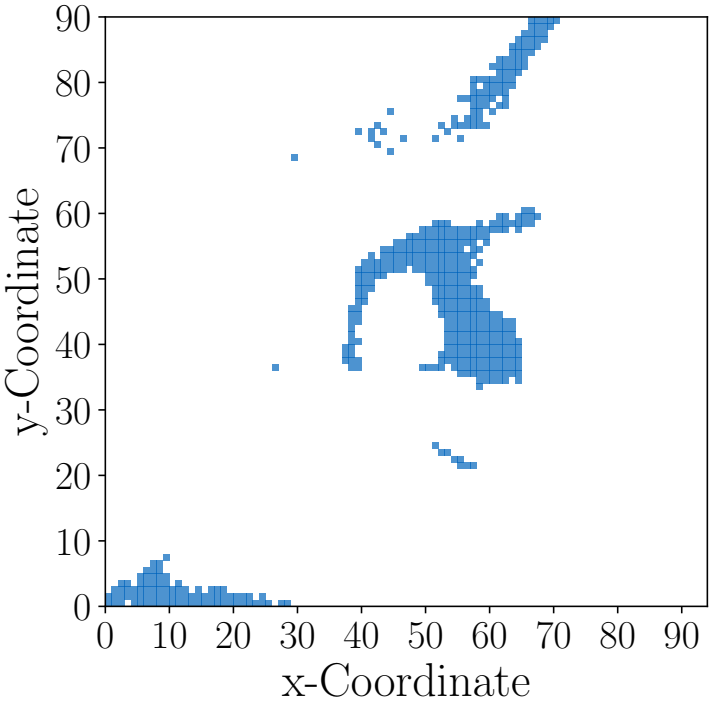
Images for $V_{Fault} = 320\,\text{V}$

Relation between EM and EMFI spots I

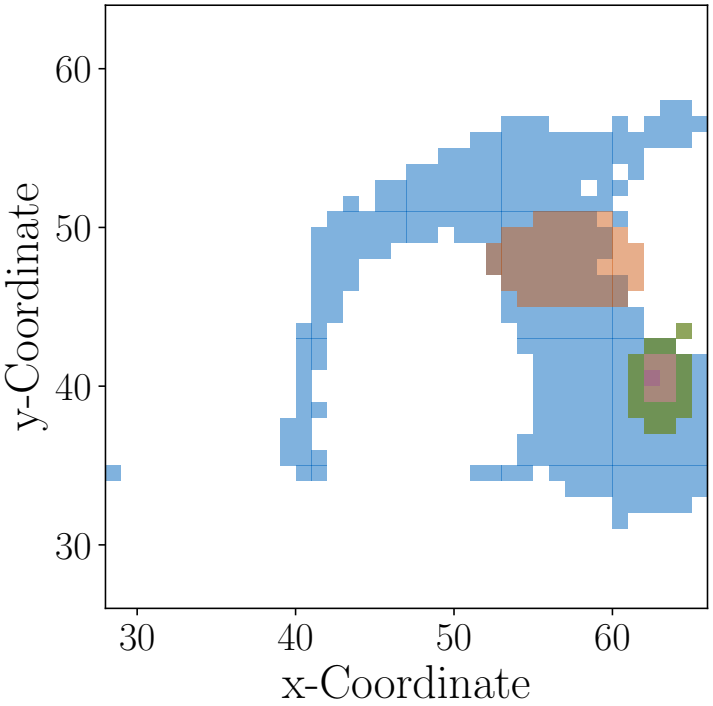


Threshold of 1.4

⇒



Relation between EM and EMFI spots II



From the figure we can see:

- (M) and most parts of (D) are included in high SNR area
- Data change area (D) is almost fully contained in the in high SNR area

This means:

→ 31% of the die area with high SNR is also prone to fault injections

→ 93% of (D) is covered by all high SNR

⇒ We can use this to speed up Sweet Spot identification

Conclusion

- ⇒ high SNR EM positions relate to fault prone positions
- ⇒ Faults only occur within the die area[1], which is 17 % of the chip area
- ⇒ We just need to inject faults at in die high SNR positions
- ⇒ By doing this, we gain a speed-up of 92.3 % (13 h instead of 168 h)

[1] in our experiments

Thank you for your attention!

matthias.probst@tum.de
https://www.sec.ei.tum.de

[1] J. Breier and D. Jap. “Testing feasibility of back-side laser fault injection on a microcontroller.” In: *Proceedings of the WESS’15: Workshop on Embedded Systems Security*. 2015, pp. 1–6.

[2] J. Danial et al. “SCNIFFER: Low-Cost, Automated, Efficient Electromagnetic Side-Channel Sniffing.” In: *IEEE Access* 8 (2020), pp. 173414–173427.

[3] M. Ghodrati et al. “Inducing local timing fault through EM injection.” In: *Proceedings of the 55th Annual Design Automation Conference*. 2018, pp. 1–6.

[4] A. Golder, A. Bhat, and A. Raychowdhury. “Exploration into the Explainability of Neural Network Models for Power Side-Channel Analysis.” In: *Proceedings of the Great Lakes Symposium on VLSI 2022*. ACM, 2022.

[5] O. M. Guillen, M. Gruber, and F. De Santis. “Low-cost setup for localized semi-invasive optical fault injection attacks: How low can we go?” In: *Constructive Side-Channel Analysis and Secure Design: 8th International Workshop, COSADE 2017, Paris, France, April 13-14, 2017, Revised Selected Papers 8*. Springer. 2017, pp. 207–222.

[6] V. V. Iyer and A. E. Yilmaz. “An Adaptive Acquisition Approach to Localize Electromagnetic Information Leakage from Cryptographic Modules.” In: *2019 IEEE Texas Symposium on Wireless and Microwave Circuits and Systems (WMCS)*. IEEE, Mar. 2019.

[7] V. V. Iyer and A. E. Yilmaz. “Rapid Pre-Characterization of Fine-Grained EM Side-Channel (In)Vulnerability of AES Modules.” In: *2022 IEEE USNC-URSI Radio Science Meeting (Joint with AP-S Symposium)*. IEEE, July 2022.

[8] R. Specht et al. “Dividing the threshold: Multi-probe localized EM analysis on threshold implementations.” In: *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, Apr. 2018.