UNIVERSIDAD
COMPLUTENSE
MADRID

Implementation of an electromagnetic fault injection platform for a RISCV-based SoC

Implementación de una plataforma para tests de inyección de fallos mediante electromagnetismo contra SoCs basados en RISC-V

2022

Realizado Por: Pedro Javier Fernández

Facultad de Informática

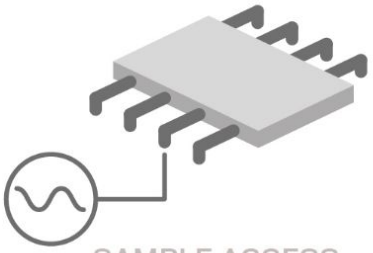
INDEX OF CONTENTS

OBJECTIVES

- **The Problem:** Spread of RISC-V. At the same time: increased need for reliable computers: in harmful conditions, but also due to rise in malicious uses of Fault Injection (FI).
- To evaluate the impact of Electromagnetic Fault Injection (EMFI) on several Systems-on-Chip (SoCs) that implement different versions of the RISC-V ISA.
- To develop an economically affordable EMFI device suited for academia research to do so.

PREVIOUS RESEARCH

Power/Clock Glitch Fault Injection (PGFI)



SAMPLE ACCESS
Only Pin access

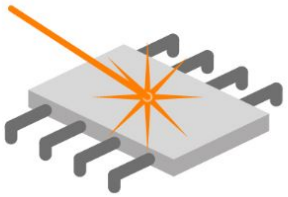
EQUIPMENT COST

PRECISION

EXPERTISE

Inject a fault by altering the clock's frequency or power supply in the corresponding pin of the chip.

Light/Laser Fault Injection (LFI)



SAMPLE ACCESS
Back side - Front side depackaging

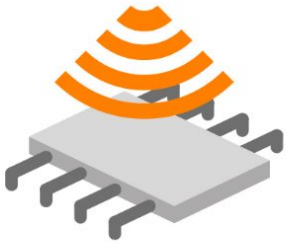
EQUIPMENT COST

PRECISION

EXPERTISE

Inject a fault by inducing a light pulse on the back side or front side surface of the silicon dice.

Electromagnetic Fault Injection (EMFI)



SAMPLE ACCESS
Front side-Back side (partial) depackaging

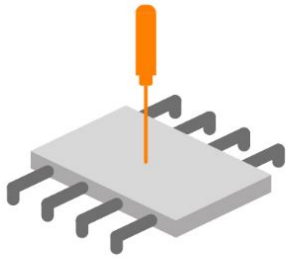
EQUIPMENT COST

PRECISION

EXPERTISE

Inject a fault by applying an electromagnetic pulse near the surface of the chip.

Body Biased Fault Injection (BBFI)



SAMPLE ACCESS
Back side depackaging

EQUIPMENT COST

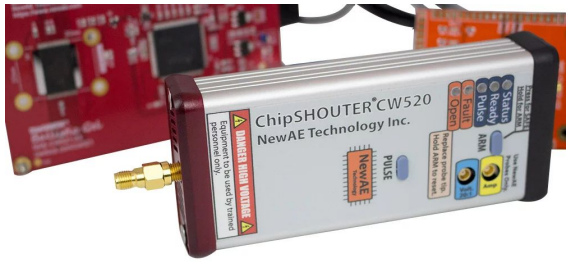
PRECISION

EXPERTISE

Inject a fault by applying a forward or reverse bias at hundred of mV to the substrate of the chip.

source: https://www.appluslaboratories.com/global/en/news/publications/new-fault-injection-attacks

PREVIOUS RESEARCH



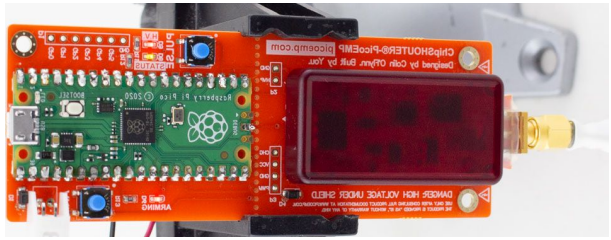
chipSHOUTER, 3000€

[1] Hajdu, N. Ivaki, I. Kocsis, “Using fault injection to assess blockchain systems in presence of faulty smart contracts,” IEEE Access, vol. 8, pp. 190760–190783, 2020

[2] EM Fault Injection on ARM and RISC-V (Mahmoud Elmohr et al.).

[3] Fault Injection on Hidden Registers in a RISC-V Rocket Processor and Software Countermeasures
Johan Laurent, V. Beroulle,

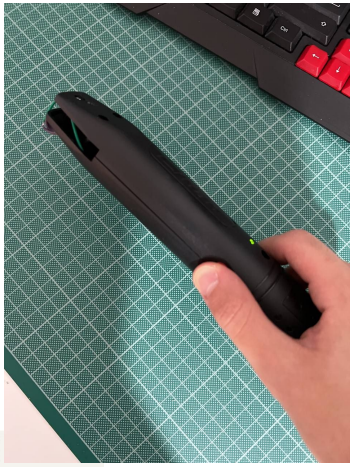
[4] PicoEMP: NewAE



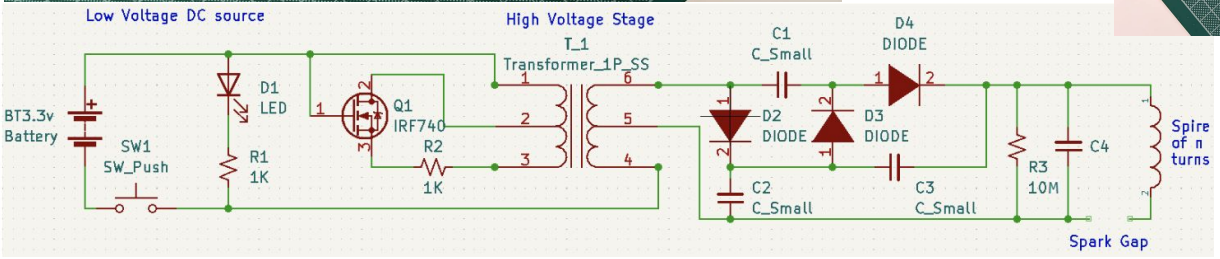
source: https://www.newae.com/auto

CONTRIBUTIONS TO EMFI

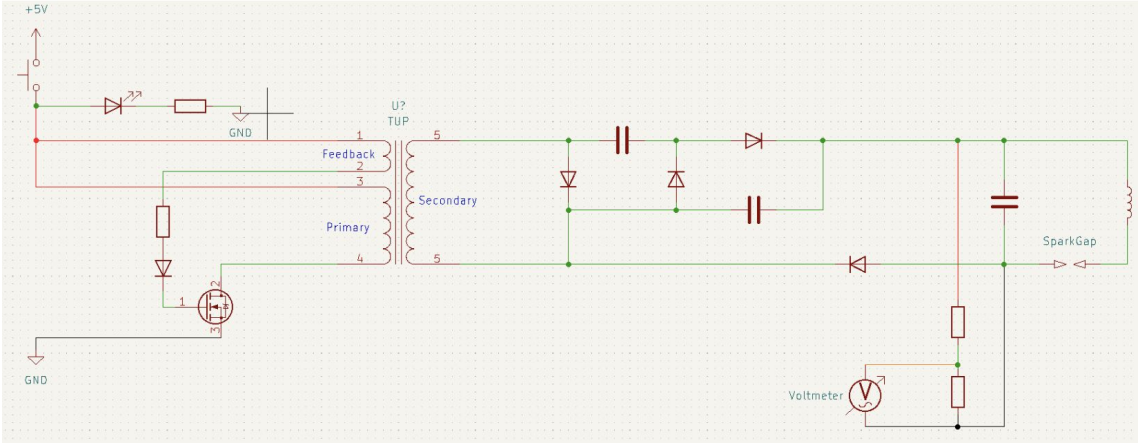
Proposal of two devices

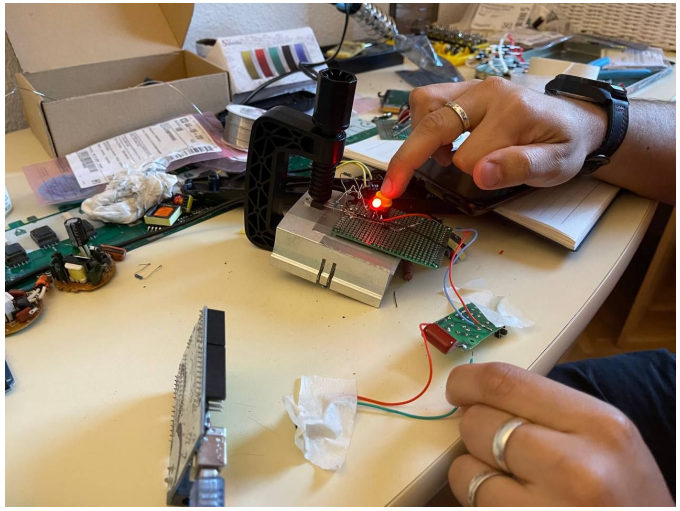


- **Device 1:** Repurposed mosquito zapper injector



- **Device 2:** *cheapSHOUTER* prototype injector



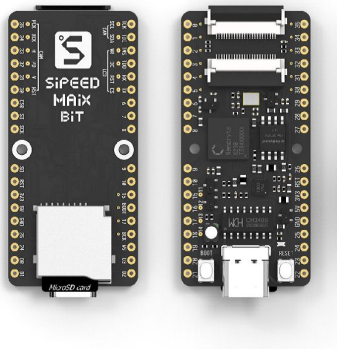


EXPERIMENTS (1)

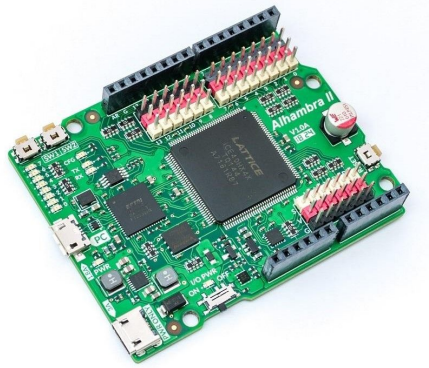
Dynamic Experiments

```c
#include <stdio.h>
int main(void){
    int i,j,k,cnt;
    k = 0;
    while(1){
     cnt = 0;
     for(i=0; i<5000; i++){
       for(j=0; j<5000; j++){
          cnt++;
       }
     }
     printf("%d %d %d %d\n", cnt, i, j,k++);
    }
}
```

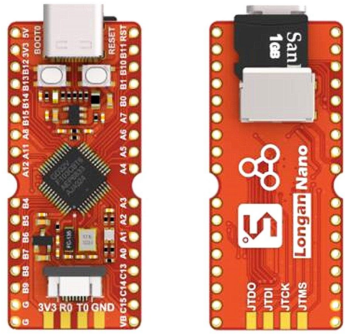
MAiX Bit (RV64GC ISA + IMAFDC)



Alhambra FPGA (RV32I soft-core)

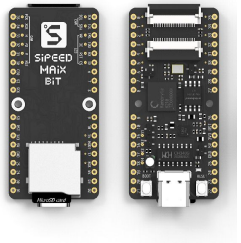


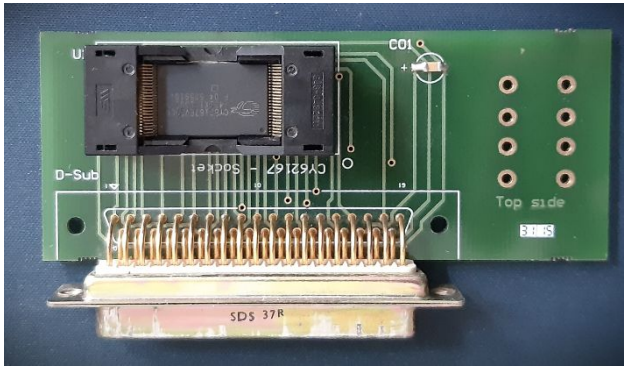
Longan Nano (RV32IMAC)



Static Experiments

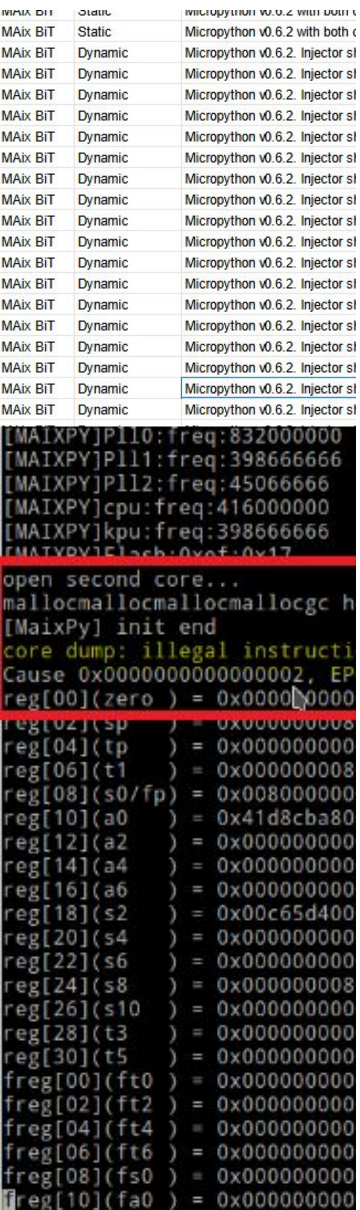
MAiX Bit with JTAG





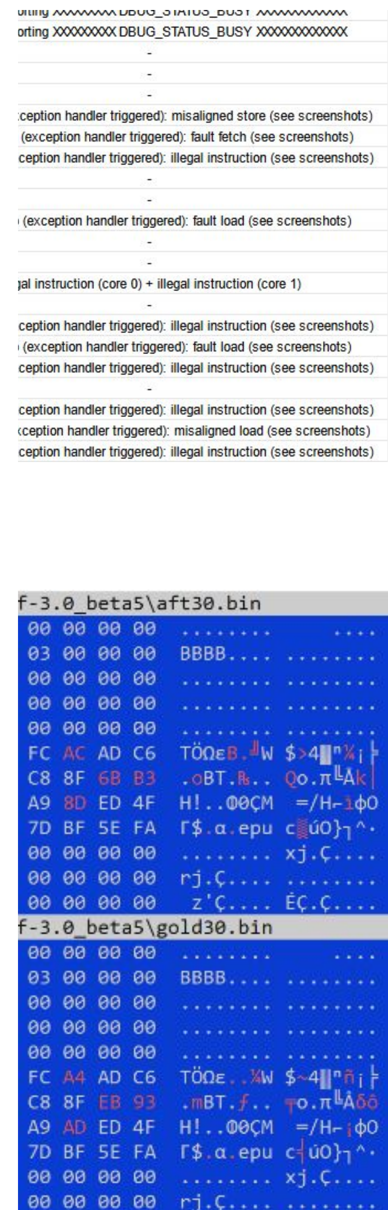
EXPERIMENTS (2)

parameters: state of the DUT, injector used, distance to the DUT, nº of shots

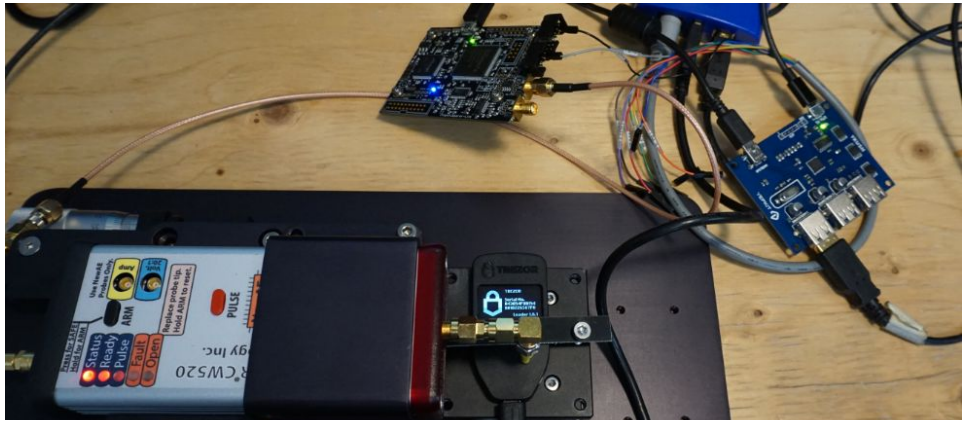


Volume II: RISC-V Privileged Architectures V1.10

Interrupt	Exception Code	Description
1	0	User software interrupt
1	1	Supervisor software interrupt
1	2	*Reserved*
1	3	Machine software interrupt
1	4	User timer interrupt
1	5	Supervisor timer interrupt
1	6	*Reserved*
1	7	Machine timer interrupt
1	8	User external interrupt
1	9	Supervisor external interrupt
1	10	*Reserved*
1	11	Machine external interrupt
1	≥12	*Reserved*
0	0	Instruction address misaligned
0	1	Instruction access fault
0	2	Illegal instruction
0	3	Breakpoint
0	4	Load address misaligned
0	5	Load access fault
0	6	Store/AMO address misaligned
0	7	Store/AMO access fault
0	8	Environment call from U-mode
0	9	Environment call from S-mode
0	10	*Reserved*
0	11	Environment call from M-mode
0	12	Instruction page fault
0	13	Load page fault
0	14	*Reserved*



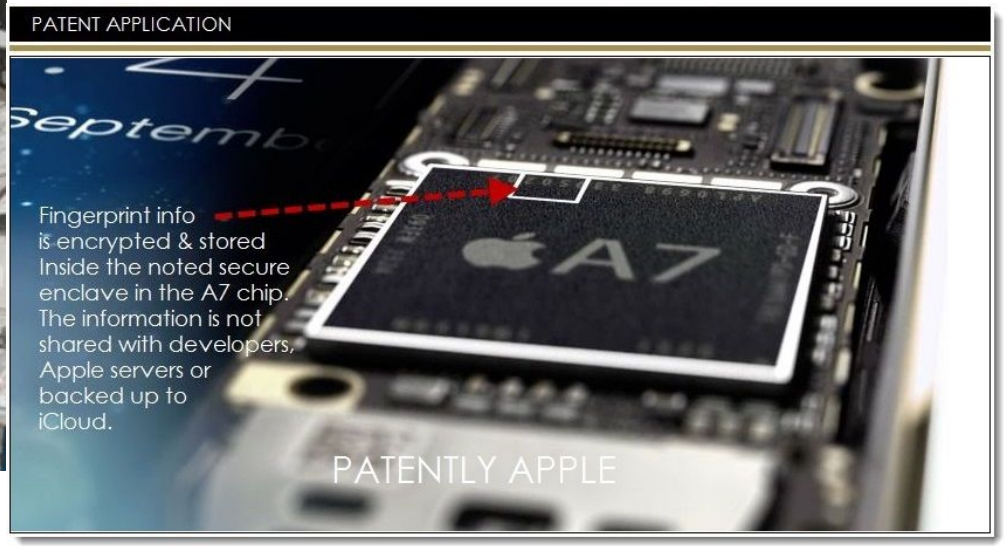
IMPACT OF THE PROPOSED SOLUTIONS

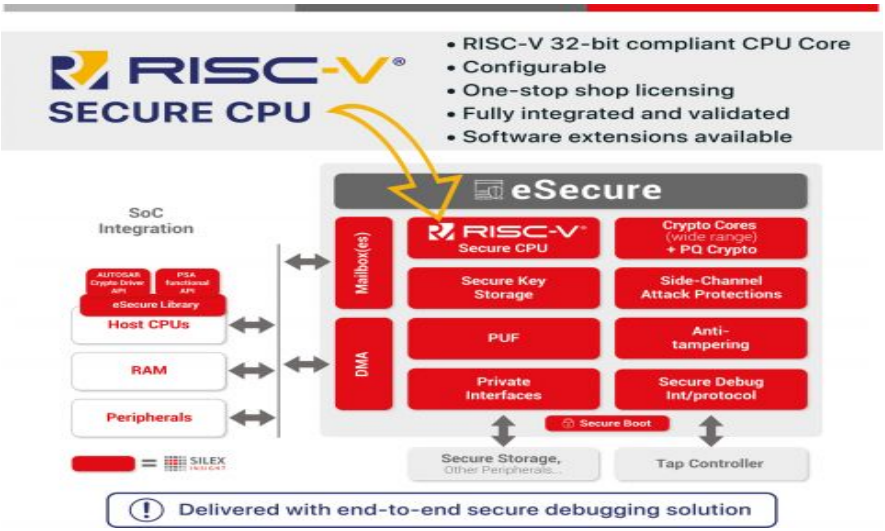


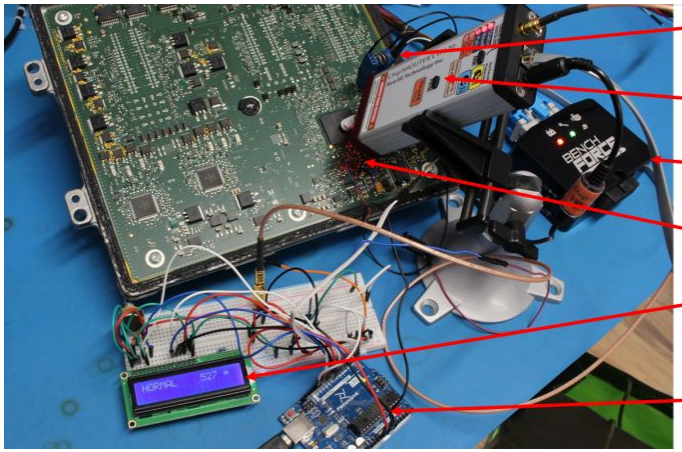
- MIN()imum Failure: EMFI Attacks against USB Stacks.Colin O'Flynn, *Dalhousie University*
- Expensive equipment requiring lots of specialization and previous research of the DUT. (i.e.: firmware reverse engineering, source code analysis, etc.)

- Low cost solution
- Enabling for less precise but much cheaper attack strategies.
- Repairable and easily accessible.
- Adequate for Devices Under Test (DUTs) and experiments in which we don’t have the need to know internal microarchitecture details.

FUTURE RESEACH LINES







source: https://www.newae.com/auto

CONCLUSIONS

- Developed an economically affordable EMFI device suited for academia research.
  - Not one but two proposed designs
- Evaluated the impact of EMFI attacks of several Systems-on-Chip (SoCs) that implement different versions of the RISC-V ISA. Causing exceptions on the DUTs. Reboots and crashes.
  - Positive results! - with room for more experimentation especially with FPGAs.
- Interesting future research topics: space computers, offensive EMFI, hardware architecture improvements, fault models, etc.

Implementación de una plataforma para tests de inyección de fallos mediante electromagnetismo contra SoCs basados en RISC-V

THANK YOU

Implementation of an electromagnetic fault injection platform for a RISCV-based SoC