EM Injection Vs. Modern CPU

Fault Characterization and AES Differential Fault Analysis

Thomas TROUCHKINE[1] **Guillaume BOUFFARD**[1,2] Jessy Clédière[3]

[1] Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
[2] DIENS, École normale supérieure, CNRS, PSL University
[3] CEA, LETI

guillaume.bouffard@ssi.gouv.fr

CEM France 2021 – 13 April 2021

Digital system usage

- Secure elements
- ✓ Certified

- High-performance component
- ✗ Not fully certified

Both are powered by System On Chips (SoCs)

System On Chip differences

Secure element

- simple CPU
- few modules
- internal memory only
- few communication interfaces

➔ Small attack surface

High-performance component

- complex CPU
- multiple modules
- internal and external memory
- multiple interfaces

➔ Large attack surface

System On Chip differences

Secure element

- simple CPU
- few modules
- internal memory only
- few communication interfaces

➔ Small attack surface

High-performance component

- complex CPU
- multiple modules
- internal and external memory
- multiple interfaces

➔ Large attack surface

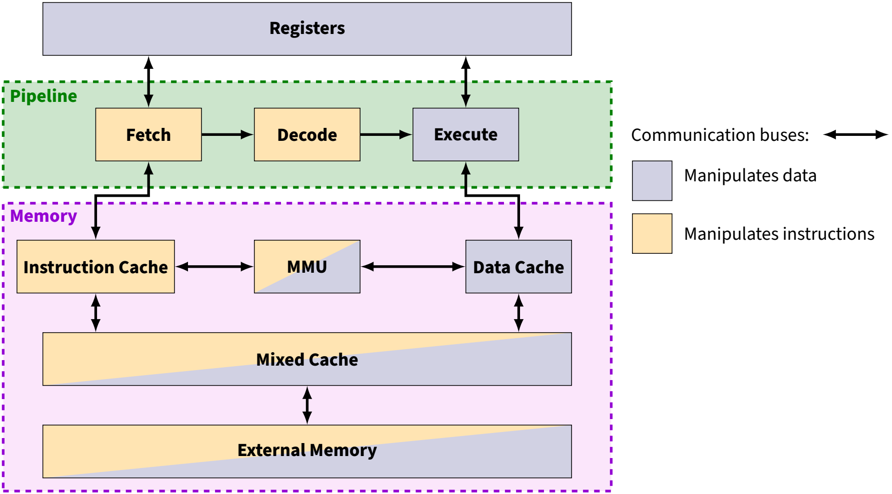
Focus on the Modern CPU **behaviour against** Fault Injections **attacks**

Complex CPU modelling overview

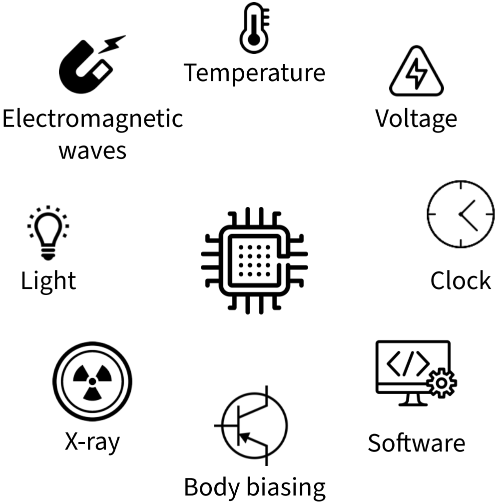
A CPU can be simplified as a set of modules:

1. A pipeline which fetches, decodes and executes instructions
2. Registers where manipulated data are temporarily stored
3. A memory to store instructions and data

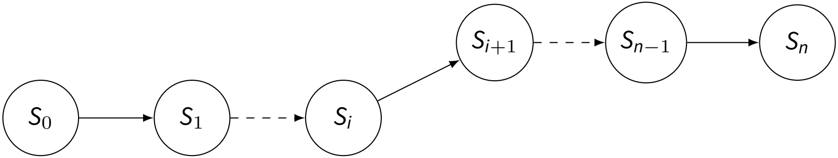
Complex CPU modelling overview (cont.)



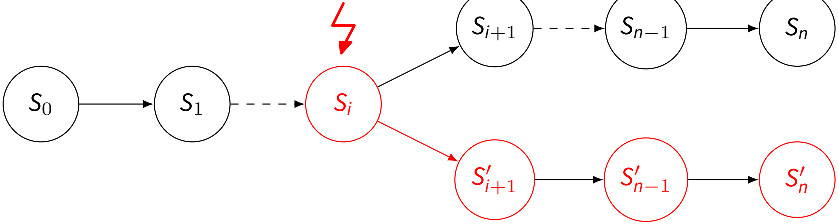
When the hardware is perturbed ...



… the software gone wild



... the software gone wild



Overview of the fault effect characterization

Injection mediums

Abstraction layer

	Clock	Voltage	EM	Laser
Program				
ISA				
Micro-architecture				

Legend: MCU's CPU SoCs' CPU FPGA Our work

Overview of the fault effect characterization

Injection mediums

Abstraction layer	Clock	Voltage	EM	Laser
Program		Forced memory ACK on MCUs [BFP19]	Control flow hijacking on ARM Cortex-M3 [BLLL18]	
ISA	Instruction skip and corruption on ATMega163 [BGV11]		Data corruption on ARM Cortex-M3 [MHD$^+$14] Instruction skip on ATMega328P [MDP$^+$20]	Instruction skip and data corruption on ATMega328P [BJ15]
ISA / Micro-architecture	Data and instruction corruption on MCUs [KH14]	Data and instruction corruption on MCUs [KH14]		
Micro-architecture	Pipeline corruption on RISC-V LEON-3 [YGS15]		Cache corruption on ARM Cortex-M4 [RNR$^+$15] Data bus corruption [MDH$^+$14] on ARM Cortex-M3 Flash corruption on MCUs [bec19, MBD$^+$19]	Flash corruption on ATMega328P [KBB$^+$18] and ARM Cortex-M3 [CMD$^+$19]

Legend: MCU's CPU | SoCs' CPU | FPGA | Our work

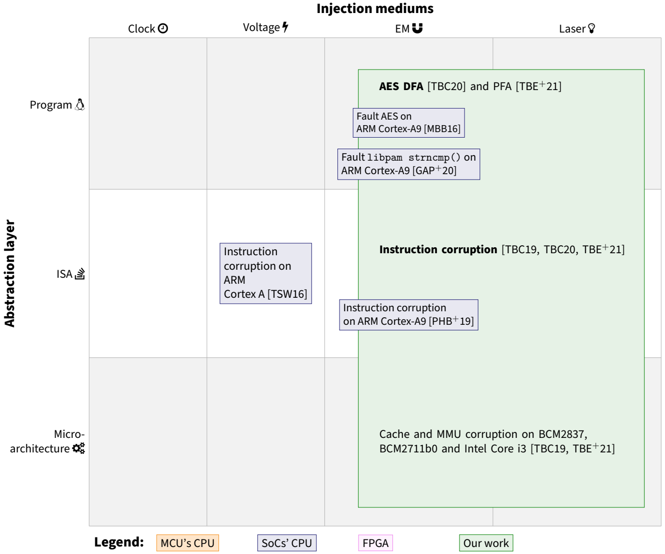
Overview of the fault effect characterization

Injection mediums

Abstraction layer	Clock	Voltage	EM	Laser
Program			Fault AES on ARM Cortex-A9 [MBB16] Fault `libpam strncmp()` on ARM Cortex-A9 [GAP+20]	
ISA		Instruction corruption on ARM Cortex A [TSW16]	Instruction corruption on ARM Cortex-A9 [PHB+19]	
Micro-architecture				

Legend: MCU's CPU SoCs' CPU FPGA Our work

Overview of the fault effect characterization



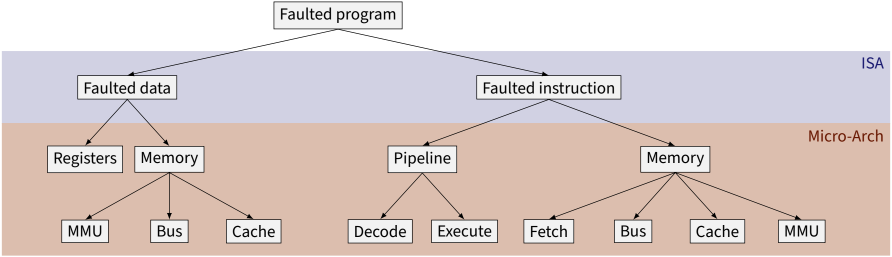
Fault effects analysis on complex CPU

During a fault, a least one micro-architectural block is perturbed

Modus operandii [TBC19]

- A test program is faulted during its execution
- Faulting various test program gives information about the micro-architectural behaviour.

Fault effects analysis on complex CPU (cont.)



Characterization Method

Test program 1

```
mov r3, r3;
/*
 * Arbitrary number
 * of repetitions
 */
mov r3, r3;
```

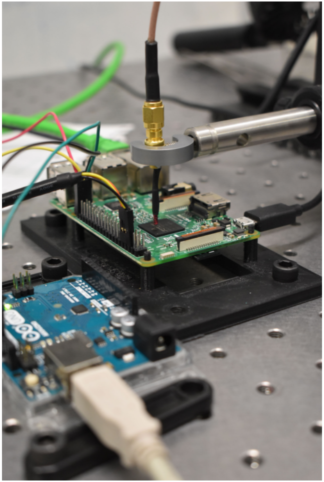
Test program 2

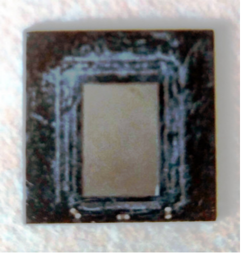
```
orr r3, r3;
/*
 * Arbitrary number
 * of repetitions
 */
orr r3, r3;
```

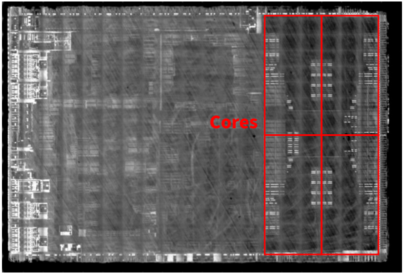
Initial values

Register	Initial values
r0	0xfffe0001
r1	0xfffd0002
r2	0xfffb0004
r3	0xfff70008
r4	0xffef0010

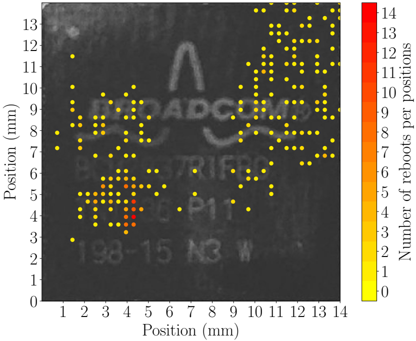
Characterization - BCM2837 (Raspberry Pi 3)



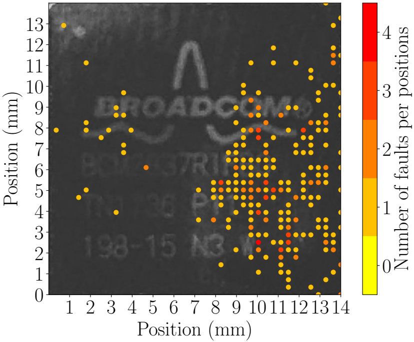




Characterization - BCM2837 (Raspberry Pi 3)



Spots leading to reboots

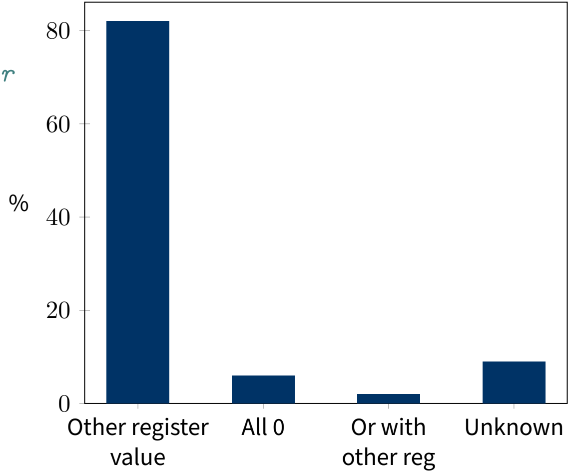


Spots leading to faults

Fault analysis on program 1

```
mov r3, r3;
/*
 * Arbitrary number
 * of repetitions
 */
mov r3, r3;
```

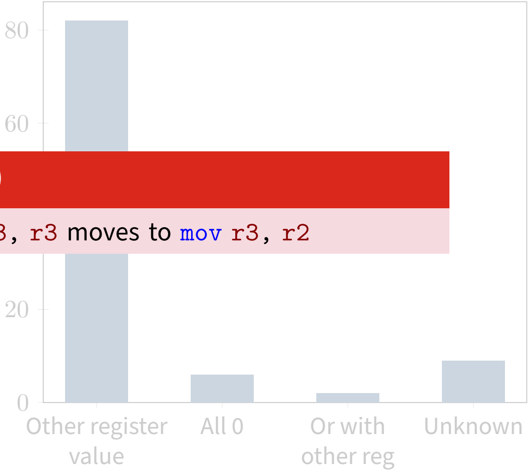
Register	Initial values
r0	0xFFFE0001
r1	0xFFFD0002
r2	0xFFFB0004
r3	0xFFF70008
r4	0xFFEF0010



Fault analysis on program 1

```
mov r3, r3;
/*
 * Arbitrary number
 * of repetitions
 */
mo
```

Regist	
r0	0xFFFE0001
r1	0xFFFD0002
r2	0xFFFB0004
r3	0xFFF70008
r4	0xFFEF0010



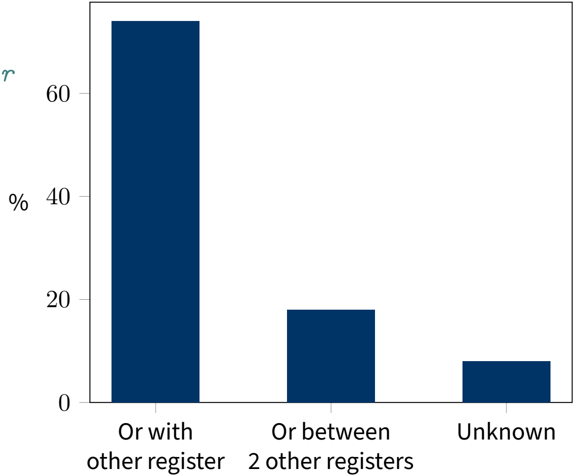
Most of time (80%)

The instruction `mov r3, r3` moves to `mov r3, r2`

Fault analysis on program 2

```
orr r3, r3;
/*
 * Arbitrary number
 * of repetitions
 */
orr r3, r3;
```

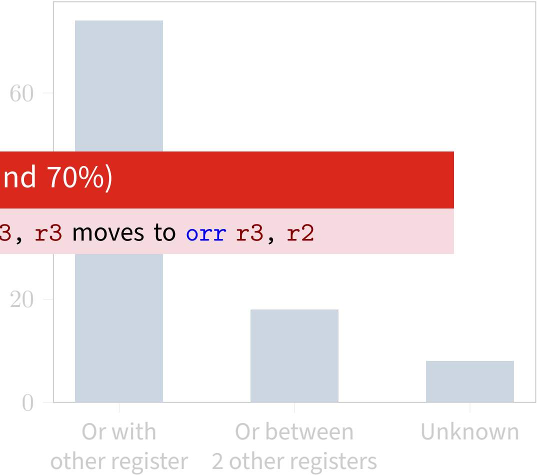
Register	Initial values
r0	0xFFFE0001
r1	0xFFFD0002
r2	0xFFFB0004
r3	0xFFF70008
r4	0xFFEF0010



Fault analysis on program 2

```
orr r3, r3;
/*
 * Arbitrary number
 * of repetitions
 */
or
```

Regist	
r0	0xFFFE0001
r1	0xFFFD0002
r2	0xFFFB0004
r3	0xFFF70008
r4	0xFFEF0010



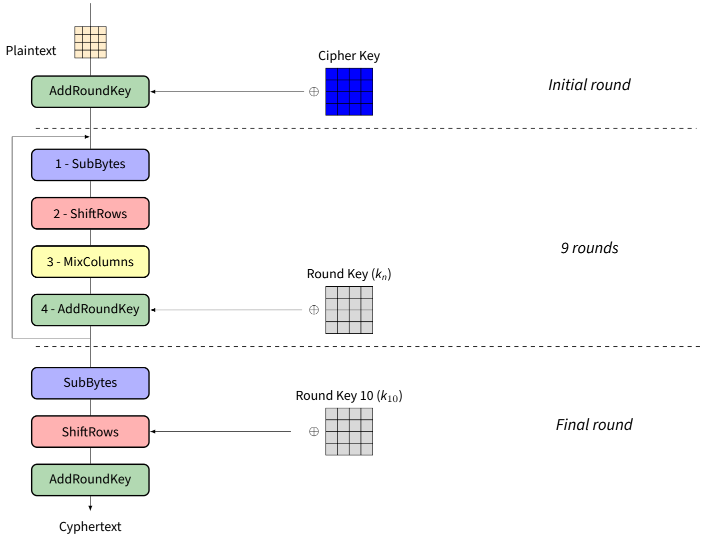
Most of time (around 70%)

The instruction `orr r3, r3` moves to `orr r3, r2`

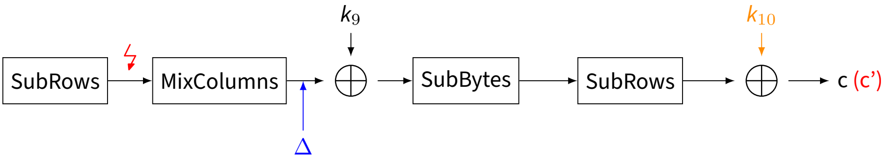
Results

- Different instructions are similarly modified
- Most of time, the second operand moves to `r2`
- Can we exploit it?

Advanced Encryption Standard (AES)

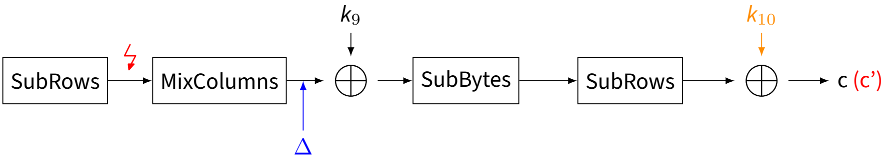


Exploitation – Differential Fault Analysis (DFA)



$$\Delta = SB^{-1}(SR^{-1}(c \oplus k_{10})) \oplus SB^{-1}(SR^{-1}(c' \oplus k_{10}))$$

Exploitation – Differential Fault Analysis (DFA)



$$\Delta = SB^{-1}(SR^{-1}(c \oplus k_{10})) \oplus SB^{-1}(SR^{-1}(c' \oplus k_{10}))$$

Setup

- OpenSSL implemention for Debian 9 on RaspberryPi3
- EMFI medium

Results

We made 3000 injections (around 1-hour required) and obtained 466 faults (15.54%):

- Only 16 (4.348%) have only one diagonal faulted => fault the cipher
  - Only 8 (50%) correspond to one byte fault before the `MixColumns` operation

Results

We made 3000 injections (around 1-hour required) and obtained 466 faults (15.54%):

- Only 16 (4.348%) have only one diagonal faulted => fault the cipher
  - Only 8 (50%) correspond to one byte fault before the `MixColumns` operation

- A suitable faulted cipher for the DFA occurs each 1/234 cipher (0.34%)
- If an injection requires 2 secondes => a suitable cipher is obtained is 10 minutes
- 3 hours of injection are needed to completely obtain to achieve the exploitation

Conclusion and future works

- From fault model analysis to exploitation
- What about fault model from ISA to complex software layout
  - Ongoing work on `sudo` program
- Reproduction-setup problem?

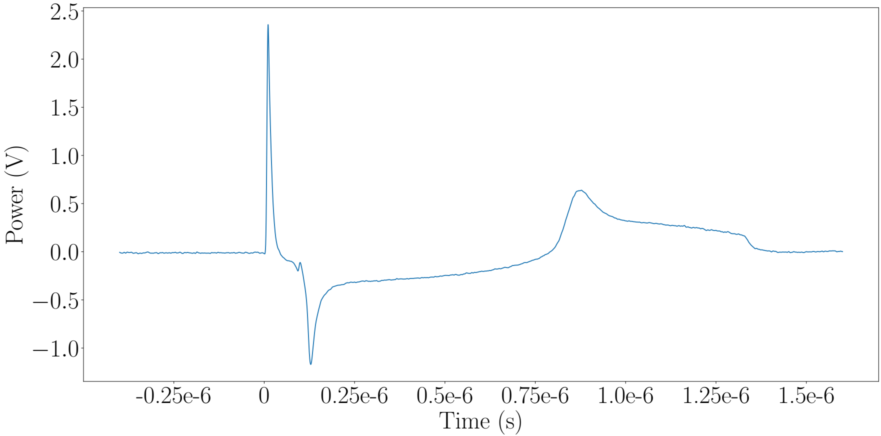
Questions?

Guillaume BOUFFARD
<guillaume.bouffard@ssi.gouv.fr>

EM injector

EM injector

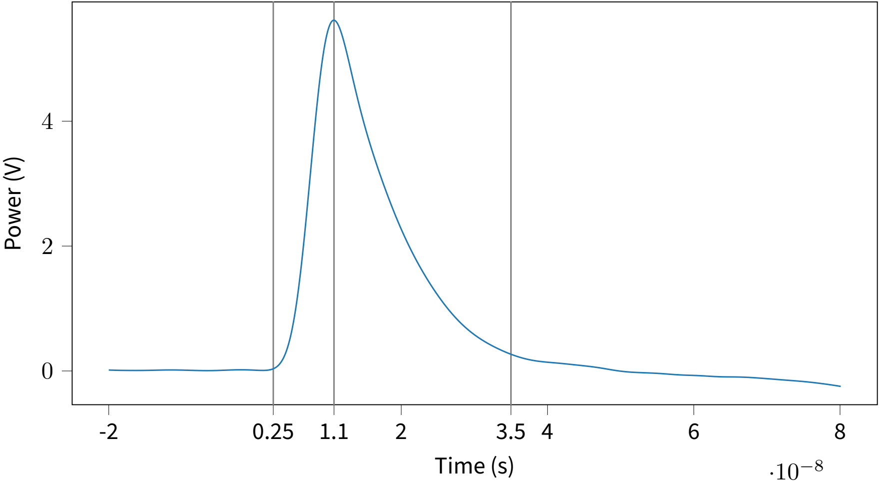
AvTec pulse generator → max 800 V/16 A



Pulse generated by the AvTech (100 V input)

EM injector

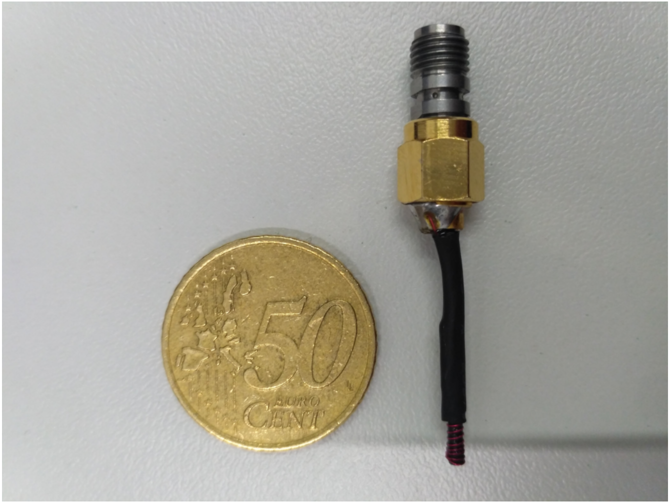
AvTec pulse generator ➞ max 800 V/16 A



Pulse generated by the AvTech zoomed on the first peak (200 V input)

EM Probe

- Home-made EMFI probe



References

[bec19] *Characterization of em faults on atmega328p*, Zenodo, July 2019.

[BFP19] Claudio Bozzato, Riccardo Focardi, and Francesco Palmarini, *Shaping the glitch: Optimizing voltage fault injection attacks*, IACR Trans. Cryptogr. Hardw. Embed. Syst. **2019** (2019), no. 2, 199–224.

[BGV11] Josep Balasch, Benedikt Gierlichs, and Ingrid Verbauwhede, *An in-depth and black-box characterization of the effects of clock glitches on 8-bit mcus*, 2011 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2011, Tokyo, Japan, September 29, 2011 (Luca Breveglieri, Sylvain Guilley, Israel Koren, David Naccache, and Junko Takahashi, eds.), IEEE Computer Society, 2011, pp. 105–114.

References (cont.)

[BJ15] Jakub Breier and Dirmanto Jap, *Testing feasibility of back-side laser fault injection on a microcontroller*, Proceedings of the 10th Workshop on Embedded Systems Security, WESS 2015, Amsterdam, The Netherlands, October 8, 2015 (Stavros A. Koubias and Thilo Sauter, eds.), ACM, 2015, p. 5.

[BLLL18] Sébanjila Kevin Bukasa, Ronan Lashermes, Jean-Louis Lanet, and Axel Legay, *Let's shock our iot's heart: Armv7-m under (fault) attacks*, Proceedings of the 13th International Conference on Availability, Reliability and Security, ARES 2018, Hamburg, Germany, August 27-30, 2018 (Sebastian Doerr, Mathias Fischer, Sebastian Schrittwieser, and Dominik Herrmann, eds.), ACM, 2018, pp. 33:1–33:6.

References (cont.)

[CMD+19] Brice Colombier, Alexandre Menu, Jean-Max Dutertre, Pierre-Alain Moëllic, Jean-Baptiste Rigaud, and Jean-Luc Danger, *Laser-induced single-bit faults in flash memory: Instructions corruption on a 32-bit microcontroller*, IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2019, McLean, VA, USA, May 5-10, 2019, IEEE, 2019, pp. 1–10.

[GAP+20] Clément Gaine, Driss Aboulkassimi, Simon Pontié, Jean-Pierre Nikolovski, and Jean-Max Dutertre, *Electromagnetic Fault Injection as a New Forensic Approach for SoCs*, IEEE WIFS 2020, 2020.

References (cont.)

[KBB+18] Dilip S. V. Kumar, Arthur Beckers, Josep Balasch, Benedikt Gierlichs, and Ingrid Verbauwhede, *An in-depth and black-box characterization of the effects of laser pulses on atmega328p*, Smart Card Research and Advanced Applications, 17th International Conference, CARDIS 2018, Montpellier, France, November 12-14, 2018, Revised Selected Papers (Begül Bilgin and Jean-Bernard Fischer, eds.), Lecture Notes in Computer Science, vol. 11389, Springer, 2018, pp. 156–170.

[KH14] Thomas Korak and Michael Hoefler, *On the effects of clock and power supply tampering on two microcontroller platforms*, 2014 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2014, Busan, South Korea, September 23, 2014 (Assia Tria and Dooho Choi, eds.), IEEE Computer Society, 2014, pp. 8–17.

References (cont.)

[MBB16] Fabien Majéric, Eric Bourbao, and Lilian Bossuet, *Electromagnetic security tests for soc*, 2016 IEEE International Conference on Electronics, Circuits and Systems, ICECS 2016, Monte Carlo, Monaco, December 11-14, 2016, IEEE, 2016, pp. 265–268.

[MBD+19] Alexandre Menu, Shivam Bhasin, Jean-Max Dutertre, Jean-Baptiste Rigaud, and Jean-Luc Danger, *Precise spatio-temporal electromagnetic fault injections on data transfers*, 2019 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2019, Atlanta, GA, USA, August 24, 2019, IEEE, 2019, pp. 1–8.

[MDH+14] Nicolas Moro, Amine Dehbaoui, Karine Heydemann, Bruno Robisson, and Emmanuelle Encrenaz, *Electromagnetic fault injection: towards a fault model on a 32-bit microcontroller*, CoRR **abs/1402.6421** (2014).

References (cont.)

[MDP+20] Alexandre Menu, Jean-Max Dutertre, Olivier Potin, Jean-Baptiste Rigaud, and Jean-Luc Danger, *Experimental analysis of the electromagnetic instruction skip fault model*, 15th Design & Technology of Integrated Systems in Nanoscale Era, DTIS 2020, Marrakech, Morocco, April 1-3, 2020, IEEE, 2020, pp. 1–7.

[MHD+14] Nicolas Moro, Karine Heydemann, Amine Dehbaoui, Bruno Robisson, and Emmanuelle Encrenaz, *Experimental evaluation of two software countermeasures against fault attacks*, 2014 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2014, Arlington, VA, USA, May 6-7, 2014, IEEE Computer Society, 2014, pp. 112–117.

References (cont.)

[PHB+19] Julien Proy, Karine Heydemann, Alexandre Berzati, Fabien Majéric, and Albert Cohen, *A first isa-level characterization of EM pulse effects on superscalar microarchitectures: A secure software perspective*, Proceedings of the 14th International Conference on Availability, Reliability and Security, ARES 2019, Canterbury, UK, August 26-29, 2019, ACM, 2019, pp. 7:1–7:10.

[RNR+15] Lionel Rivière, Zakaria Najm, Pablo Rauzy, Jean-Luc Danger, Julien Bringer, and Laurent Sauvage, *High precision fault injections on the instruction cache of armv7-m architectures*, IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2015, Washington, DC, USA, 5-7 May, 2015, IEEE Computer Society, 2015, pp. 62–67.

[TBC19] Thomas Trouchkine, Guillaume Bouffard, and Jessy Clediere, *Fault Injection Characterization on modern CPUs – From the ISA to the Micro-Architecture*, WISTP 2019, Paris, France, 2019.

References (cont.)

[TBC20] _______, *Em injection vs. modern cpu - fault characterization and aes differential fault analysis*, Comptatibilité électromagnétique France 2020, 2020.

[TBE+21] Thomas Trouchkine, Sébanjila Kevin Bukasa, Mathieu Escouteloup, Ronan Lashermes, and Guillaume Bouffard, *Electromagnetic fault injection against a complex cpu, toward a new micro-architectural fault models*, Journal of Cryptographic Engineering (JCEN), 2021.

[TSW16] Niek Timmers, Albert Spruyt, and Marc Witteman, *Controlling PC on ARM using fault injection*, 2016 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2016, Santa Barbara, CA, USA, August 16, 2016, IEEE Computer Society, 2016, pp. 25–35.

References (cont.)

[YGS15] Bilgiday Yuce, Nahid Farhady Ghalaty, and Patrick Schaumont, *Improving fault attacks on embedded software using RISC pipeline characterization*, 2015 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2015, Saint Malo, France, September 13, 2015 (Naofumi Homma and Victor Lomné, eds.), IEEE Computer Society, 2015, pp. 97–108.