Targeting several unpipelined instructions with a single EM pulse on 8-bit MCU

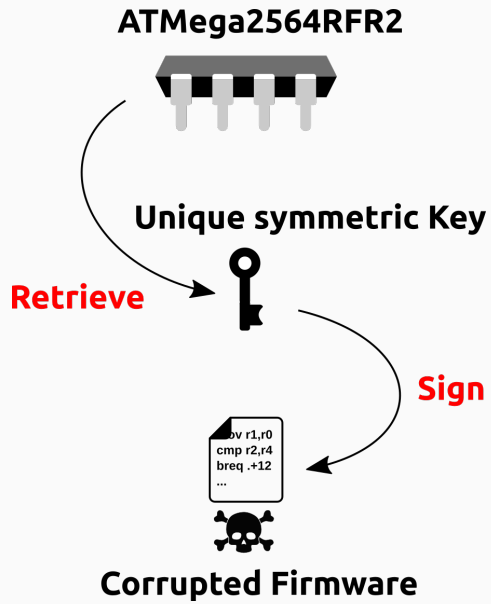
Cryptarchi, June 18th, 2018

[1]A. Menu, [2]J-L. Danger, [1]J-M. Dutertre,
[1]E. Kharbouche, [1]O. Potin, [1]J-B. Rigaud

[1]Ecole des Mines de Saint-Etienne, {prenom}.{nom}@emse.fr
[2]Telecom Paristech, {prenom}.{nom}@telecom-paristech.fr

Summary

1. Context
2. Analysis of EM injection parameters
3. Skipping several consecutive instructions
4. Bypassing a secured verifyPIN
5. Conclusion

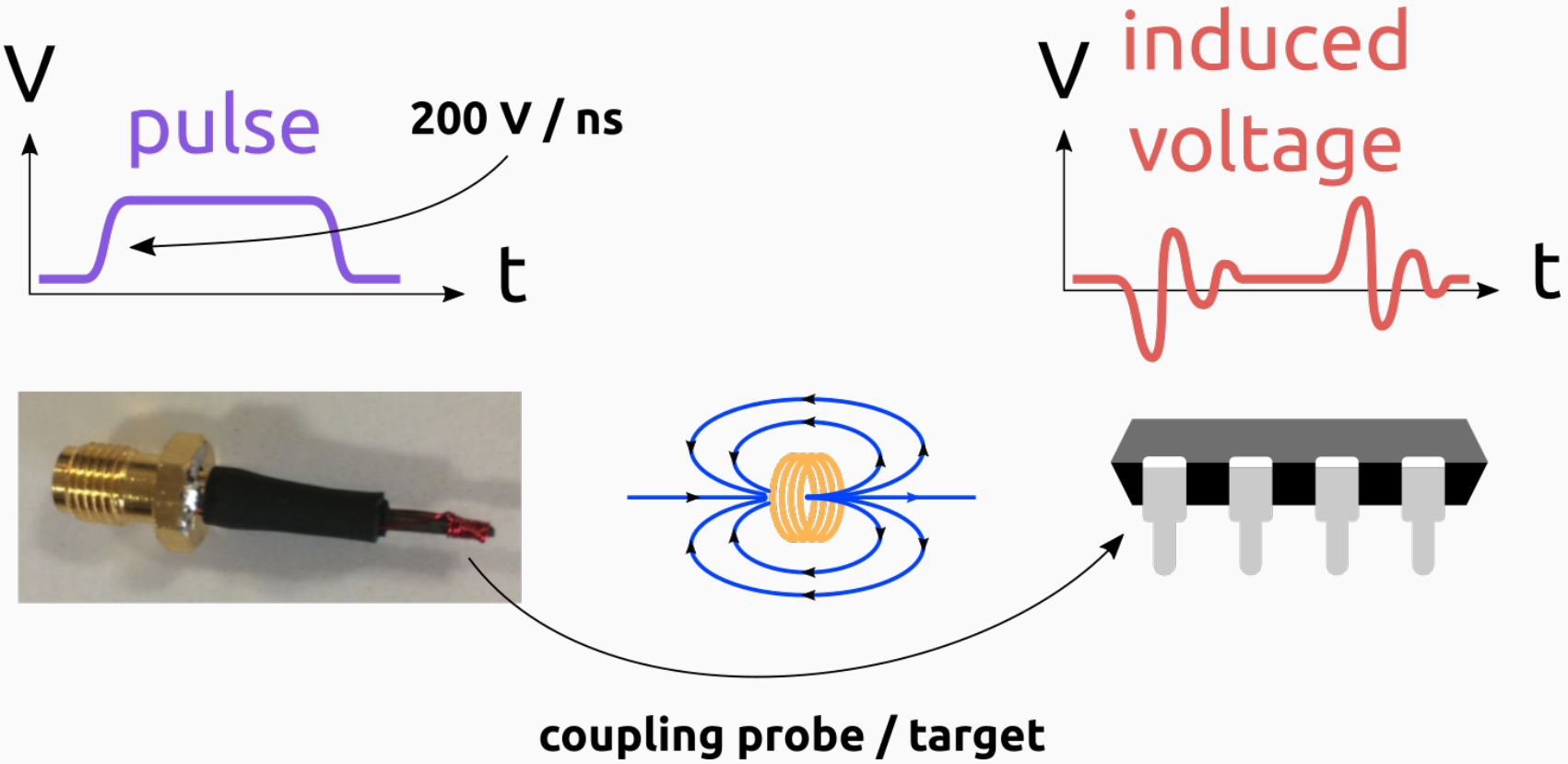


Side channel attack vectors in IoT [Ronen'16]

Context

EM fault injection

Physical principle: Lenz-Faraday Law



EM fault injection

Benefits of EM injection

- ✓ **non-invasive** [Schmidt'07]
- ✓ **local** [Poucheret'11, Chusseau'14]
- ✓ **precise and reproducible** [Dehbaoui'12]

Balance precision / equipment cost & human investment

EM fault injection

EM fault models

- how to distinguish fault on data flow and control flow ? [Dehbaoui'12, Moro'13]
- how to observe a given fault model ? [Dureuil'16]

	control flow				data flow	
	Replay	Instr. skip	Opcode corruption	PC corruption	Monobyte fault	monobit fault
Schmidt'07		?	?	?		
Dehbaoui'12		✓	?	?	✓	
Moro'13		✓	✓	✓	✓	
Rivière'15	✓					

Non-exhaustive review of observed EM fault models

EM fault injection

Our research direction: **instruction skip** fault model

- target both control and data flow
- easy to induce leveraging EM injection

EM fault injection

Single Instruction skip on 8-bit and 32-bit MCU

- a relatistic fault model [Schmidt'08, Barenghi'09, Balasch'11, Breier'15]
- well known in fault simulation and counter-measure design [Rivière'14, Moro'14, Barry'17]

Multiple consecutive instruction skips ?

- Fault on cache read (instruction replay) [Rivière'15]
- clock glitch on pipelined architecture [Yuce'16]

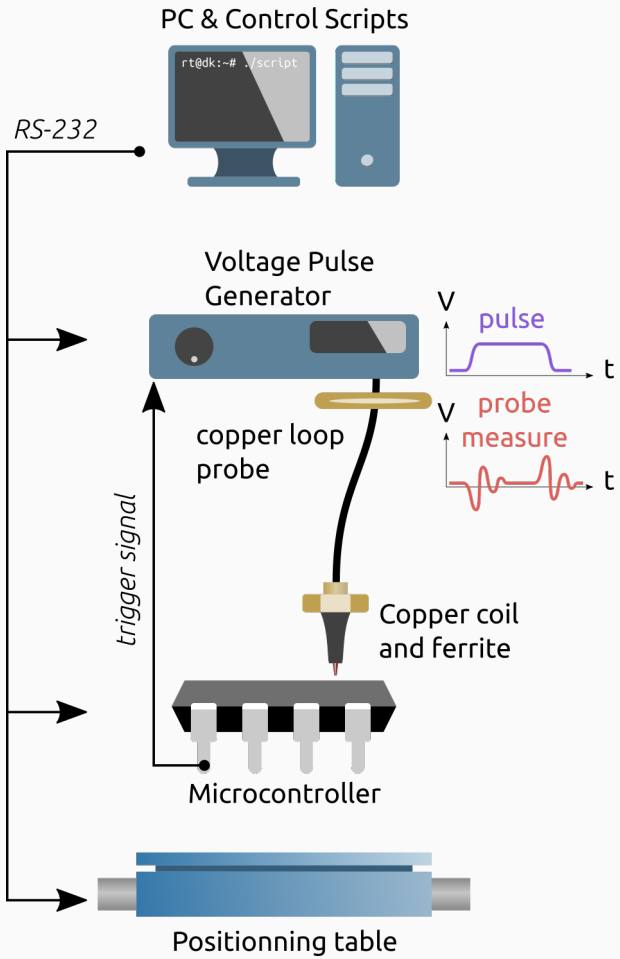
Contribution:

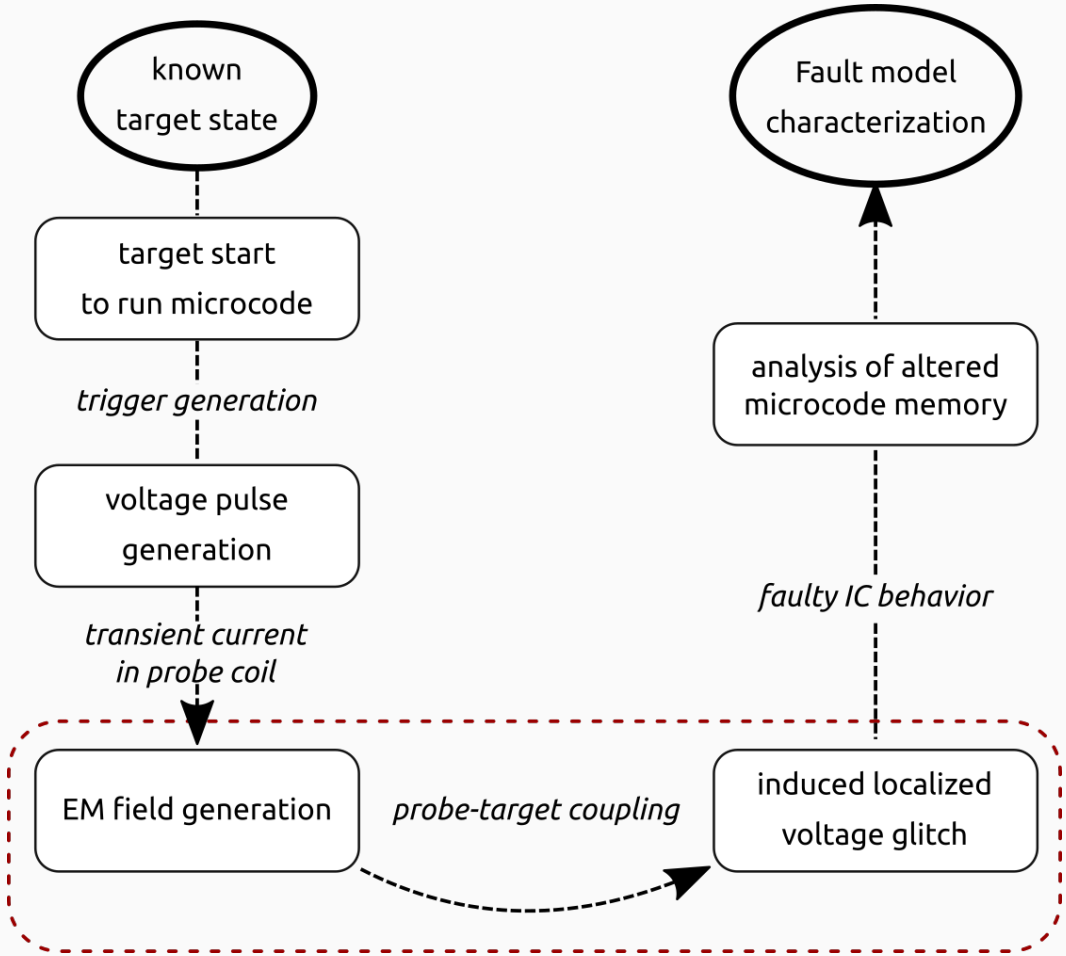
How realistic is the EM induced multiple consecutive skips fault model ?

Analysis of EM injection parameters

Analysis of EM injection parameters

Experimental setup and methodology

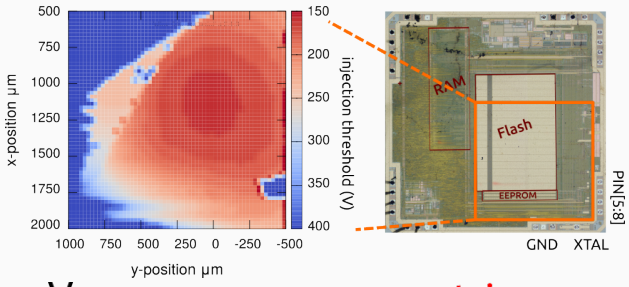


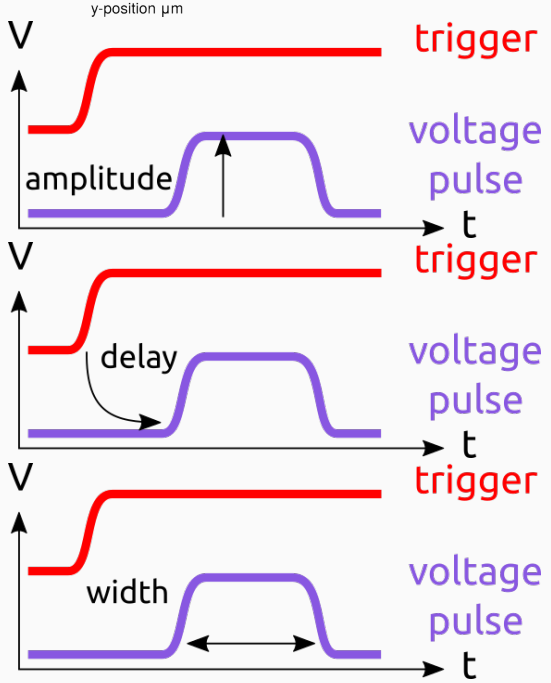


Analysis of injection parameters

Experimental parameters

- Probe location (x, y, z)
- Pulse amplitude
- Delay or Injection timing
- Pulse width





⚠ **Main challenge: combinatorial explosion !** ⚠

Analysis of injection parameters

Fault model characterization

- Do we retrieve initialization value ?
- Does the execution time change ?
  ($T_{LOAD} = 2T_{NOP}$)

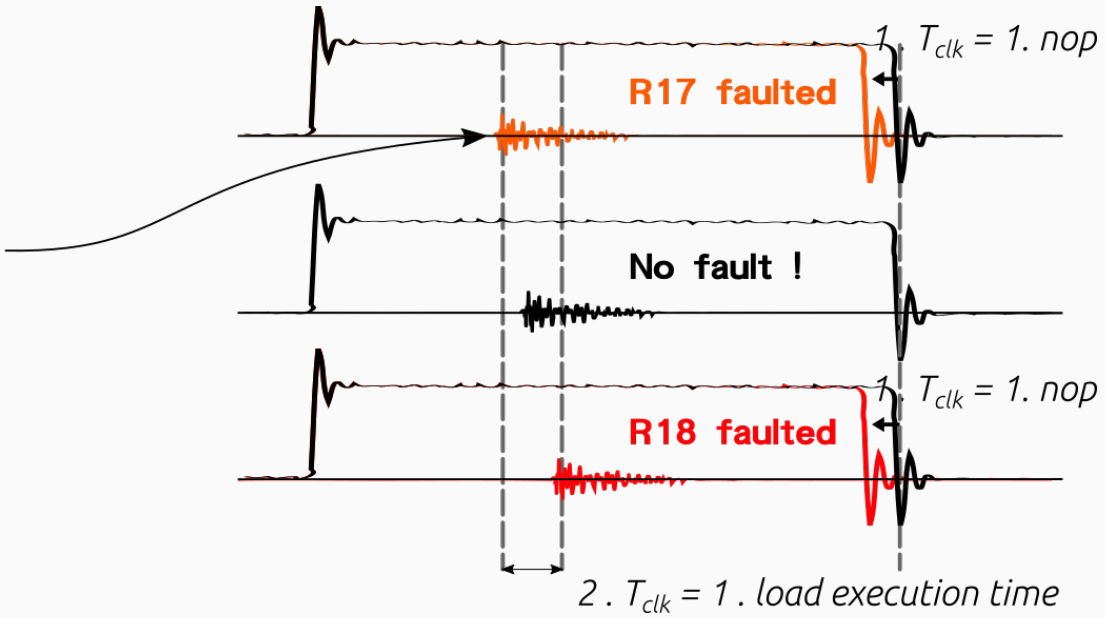
```
#start
ld r16, 0x55
...
ld r25, 0x55

#rise trigger
ld r16, 0x39
ld r17, 0x38
...
ld r25, 0x30
#clear trigger

#readback
mov %[reg16], r16
...
mov %[reg25], r25
#end
```

Analysis of injection parameters

EM specific fault mecanism

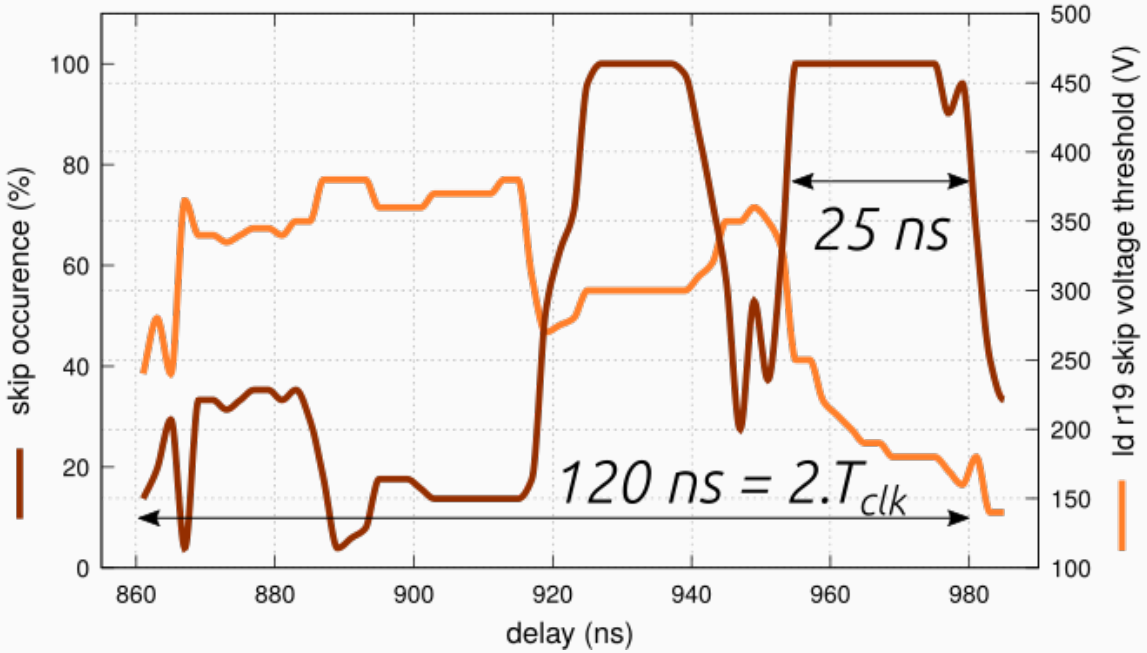
```
#start
#init with 0x55

#rise trigger
ld r16, 0x39
ld r17, 0x38
ld r18, 0x37
...
#clear trigger

#readback
#39 38 37 36 35
#34 33 32 31 30
#end
```

```
#start
#init with 0x55

#rise trigger
ld r16, 0x39
nop
ld r18, 0x37
...
#clear trigger

#readback
#39 55 37 36 35
#34 33 32 31 30
#end
```



Analysis of injection parameters

The **injection threshold** is defined as the minimum pulse amplitude, which induces an instruction skip

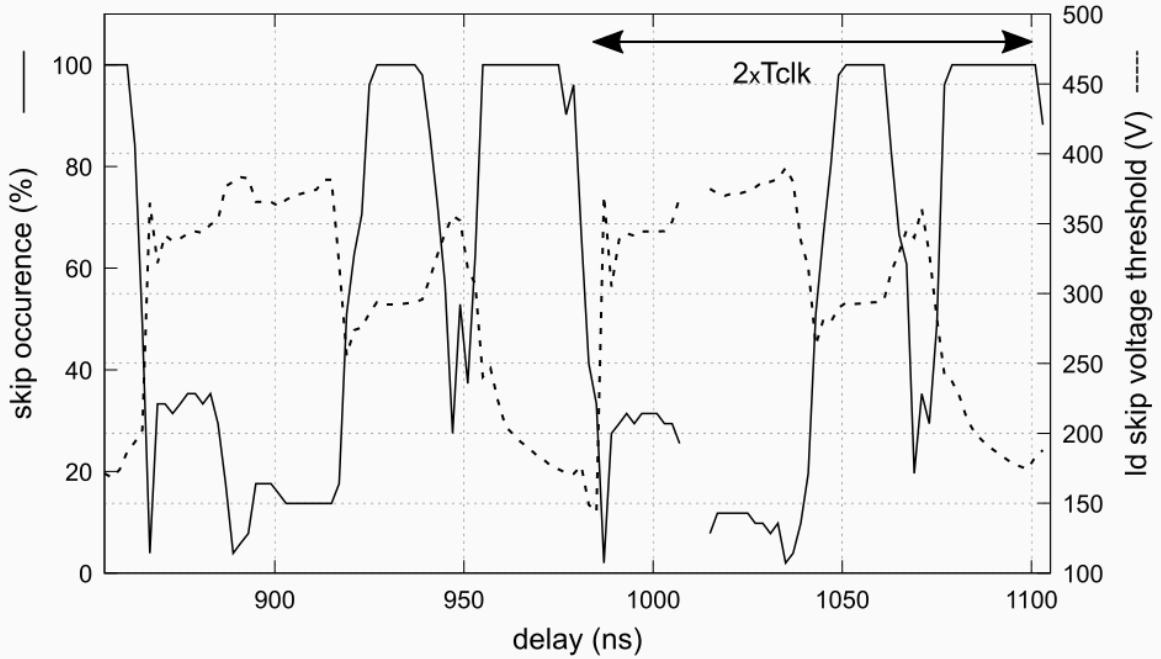


ld r19, 0x36

One should target susceptibility windows [Ordas'15]

Analysis of injection parameters

Peridodicity of temporal sensitivity

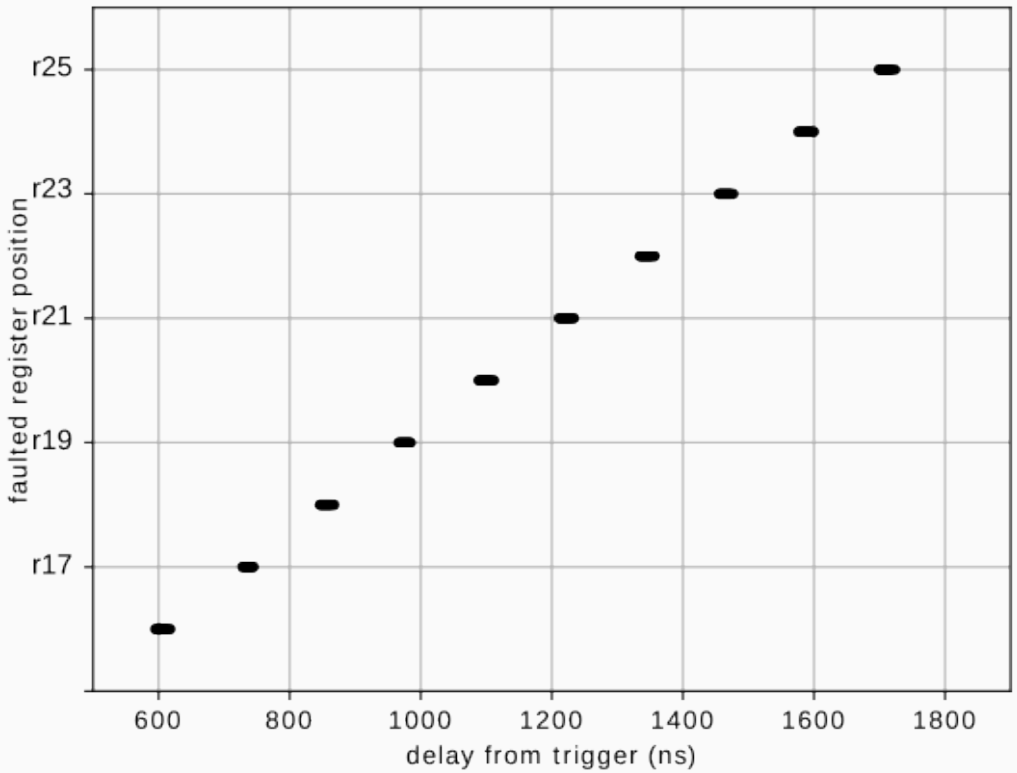


ld r19, 0x36; ld r20, 0x35

Take should be taken of the injection timing accuracy

Analysis of injection parameters

Targeting a single instruction (amplitude, injection timing)



Same level of control as laser injection [Breier'15]

Analysis of injection parameters

Wrapping up:

- Understanding the influence of EM injection parameters
- Targeted single instruction skip (delay, amplitude)
- Reproducible skip in susceptibility windows

Skipping several consecutive instructions

Skipping several consecutive instructions

Pulse width influence ?

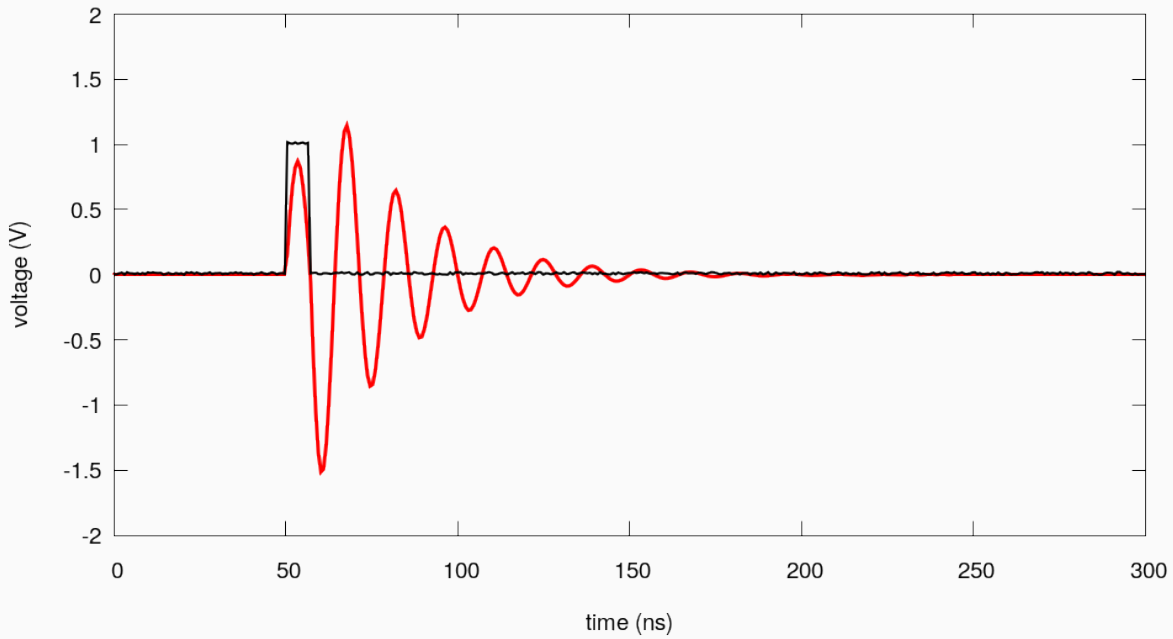
Qualitative observations:

- **long** pulse lead to stress attenuation [Moro'13]
- **very short** pulse lead to stress attenuation

Skipping several consecutive instructions

Hypothesis : damped wave packets on power-ground network (PGN)

- Probe / PGN coupling [Poucheret'11]
- voltage glitch on PGN [Zussa'14]

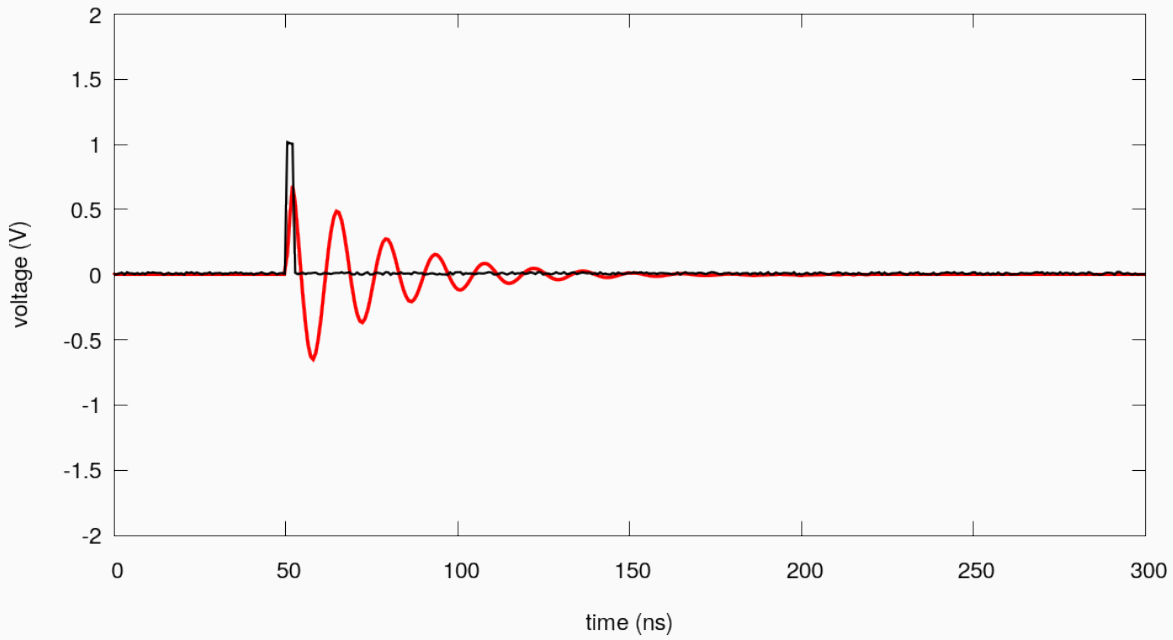


Constructive interferences (min. at -1.5 V)

Skipping several consecutive instructions

Hypothesis : damped wave packets on power-ground network (PGN)

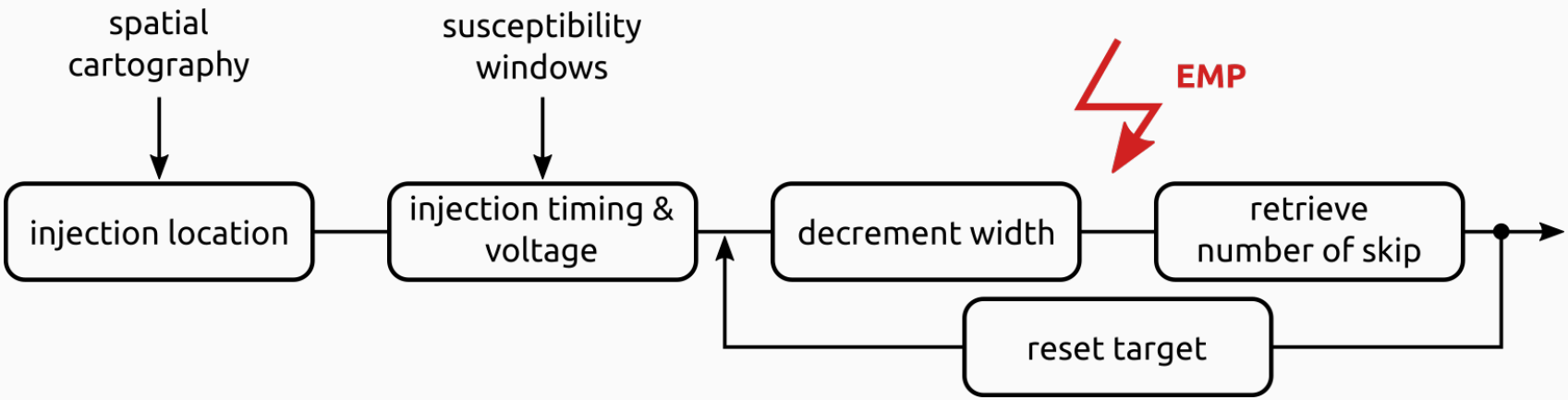
- Probe / PGN coupling [Poucheret'11]
- voltage glitch on PGN [Zussa'14]



Destructive interferences (min. below -1 V)

Skipping several consecutive instructions

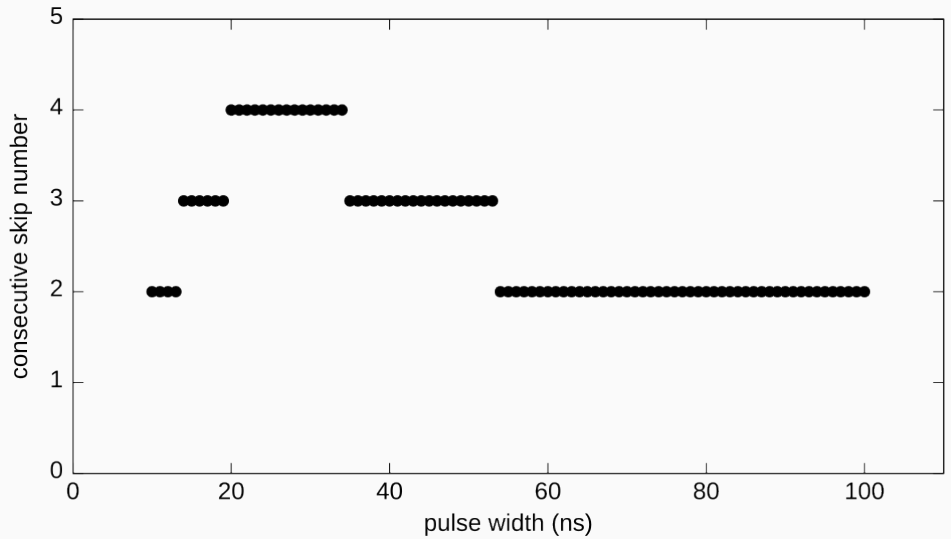
Characterization methodology of width influence:



Skipping several consecutive instructions

Hypothesis : damped wave packets on power-ground network (PGN)

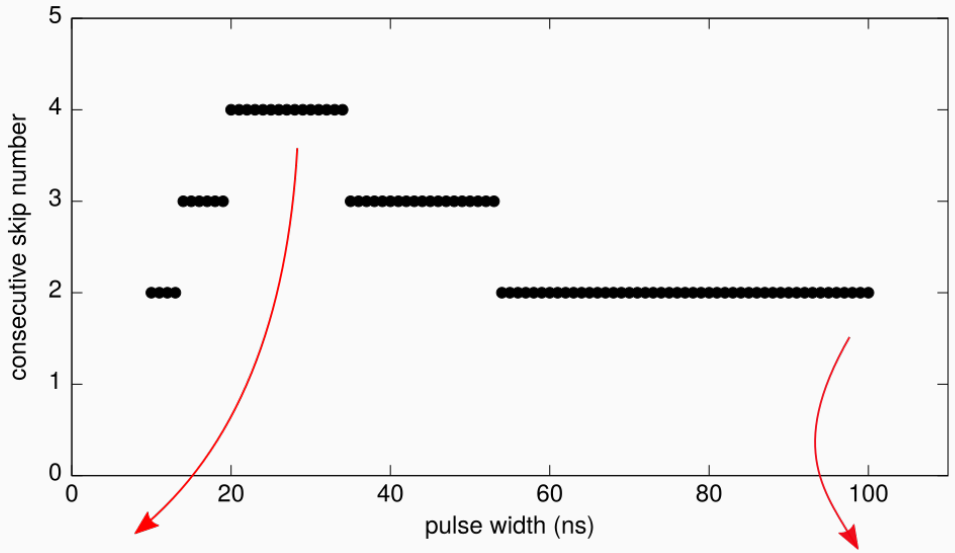
- destructives interferences $w < 20$ *ns*
- constructive interferences $w \approx 25$ *ns*
- no interferences $w > 50$ *ns*

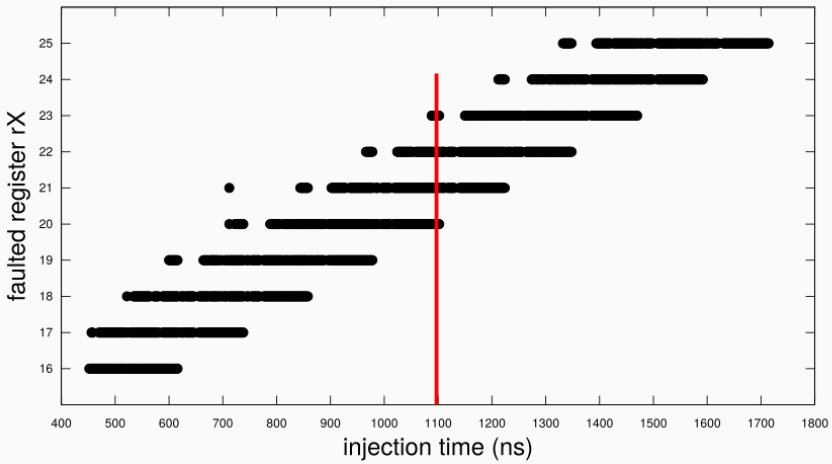


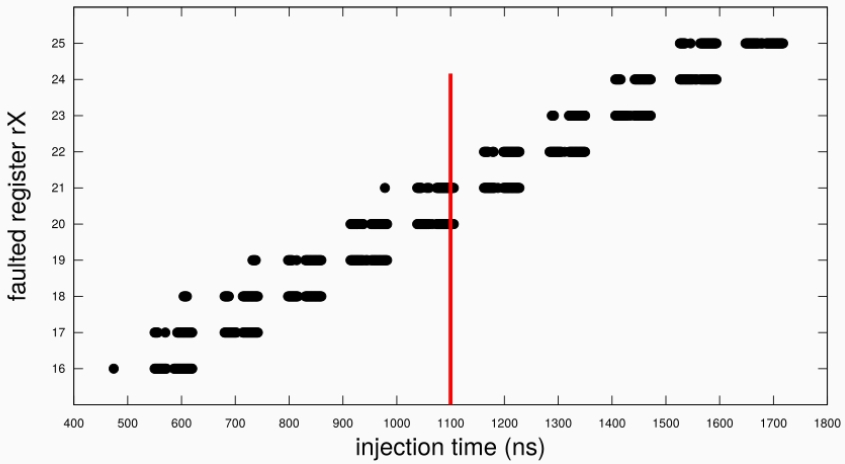
Are we still able to select a given instruction ?

Skipping sevseral consecutive instructions

Targeting a specific instruction block (width, timing)







Bypassing a secured verifyPIN

Practical case: bypassing a secured verifyPIN

Duplication countermeasure on non-secured atmega328p

```
#define BOOL_TRUE 0XAA
#define BOOL_FALSE 0X55

void verifyPIN(){
    g_authenticated =BOOL_FALSE;
    if(g_ptc > 0){
        g_ptc--;
        if(byteArrayCompare(g_userPin, g_cardPin) == BOOL_FALSE){
            g_ptc = 3 ;
            g_authenticated = BOOL_TRUE ;
        }
    }
}
```

TEST DUPLICATION

```
#skip auth. if incorrect
#pin provided
cpi r17, 0x55
brne .+8
cpi r17, 0x55
brne .+4
ldi r20, 0x03
ldi r16, 0xAA

#store value in RAM
sts 0X01A9, r20
sts 0X01AA, r16
sts 0X01A9, r20
sts 0X01AA, r16
```

Practical case: bypassing a secured verifyPIN

injection parameters: voltage = -350 V, width = 25 ns

```
#define BOOL_TRUE 0XAA
#define BOOL_FALSE 0X55

void verifyPIN(){
    g_authenticated =BOOL_FALSE;
    if(g_ptc > 0){
        g_ptc--;
        if(byteArrayCompare(g_userPin, g_cardPin) == BOOL_FALSE){
            g_ptc = 3 ;
            g_authenticated = BOOL_TRUE ;
        }
    }
}
```

TEST DUPLICATION

#skip auth. if incorrect
#pin provided

4 skips

```
ldi r20, 0x03
ldi r16, 0xAA

#store value in RAM
sts 0X01A9, r20
sts 0X01AA, r16
sts 0X01A9, r20
sts 0X01AA, r16
```

Conclusion

Conclusion

Our methodology allowed us to fault:

- A specific instruction (amplitude, timing)
- Or a specific number of instructions (pulse width, timing)
- In a reproductible manner (amplitude, timing)

A fine grain width/timing adjustment is required

Next steps

- Can it be extent to 32-bit architectures ?
- External syncronization ?
- Attack of secure boot implementation ? [Timmers'16]

Thanks for your attention !

alexandre.menu@emse.fr

References

[1] J. Balasch, B. Gierlichs, and I. Verbauwhede. An in-depth and black-box characterization of the effects of clock glitches on 8-bit mcus. In *2011 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 105–114, Sept 2011.

[2] A. Barenghi, G. Bertoni, E. Parrinello, and G. Pelosi. Low voltage fault attacks on the rsa cryptosystem. In *2009 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 23–31, Sept 2009.

References ii

[3] T. Barry, D. Couroussé, and B. Robisson. Compilation of a countermeasure against instruction-skip fault attacks. In *Proceedings of the Third Workshop on Cryptography and Security in Computing Systems*, CS2 '16, pages 1–6, New York, NY, USA, 2016. ACM.

[4] J. Breier, D. Jap, and C.-N. Chen. Laser profiling for the back-side fault attacks: With a practical laser skip instruction attack on aes. In *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, CPSS '15, pages 99–103, New York, NY, USA, 2015. ACM.

References iii

[5] L. Chusseau, R. Omarouayache, J. Raoult, S. Jarrix, P. Maurine, K. Tobich, A. Bover, B. Vrignon, J. Shepherd, T. H. Le, M. Berthier, L. Rivière, B. Robisson, and A. L. Ribotta. Electromagnetic analysis, deciphering and reverse engineering of integrated circuits (e-mata hari). In *2014 22nd International Conference on Very Large Scale Integration (VLSI-SoC)*, pages 1–6, Oct 2014.

[6] A. Dehbaoui, J. M. Dutertre, B. Robisson, and A. Tria. Electromagnetic transient faults injection on a hardware and a software implementations of aes. In *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 7–15, Sept 2012.

[7] L. Dureuil. *Code analysis and evaluation process for vulnerability detection against fault injection on secure hardware*. Theses, Université Grenoble Alpes, Oct. 2016.

References iv

[8] J. marc Schmidt and M. Hutter. Optical and em fault-attacks on crt-based rsa: Concrete results, 2007.

[9] N. Moro, A. Dehbaoui, K. Heydemann, B. Robisson, and E. Encrenaz. Electromagnetic fault injection: Towards a fault model on a 32-bit microcontroller. In *2013 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 77–88, Aug 2013.

[10] N. Moro, K. Heydemann, A. Dehbaoui, B. Robisson, and E. Encrenaz. Experimental evaluation of two software countermeasures against fault attacks. In *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pages 112–117, May 2014.

[11] S. Ordas, L. Guillaume-Sage, and P. Maurine. Em injection: Fault model and locality. In *2015 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 3–13, Sept 2015.

References v

[12] F. Poucheret, L. Chusseau, B. Robisson, and P. Maurine. Local electromagnetic coupling with cmos integrated circuits. In *2011 8th Workshop on Electromagnetic Compatibility of Integrated Circuits*, pages 137–141, Nov 2011.

[13] L. Rivière, M.-L. Potet, T.-H. Le, J. Bringer, H. Chabanne, and M. Puys. Combining High-Level and Low-Level Approaches to Evaluate Software Implementations Robustness Against Multiple Fault Injection Attacks. In *Foundations and Practice of Security*, Montreal, Canada, Nov. 2014.

[14] L. Rivière, Z. Najm, P. Rauzy, J.-L. Danger, J. Bringer, and L. Sauvage. High Precision Fault Injections on the Instruction Cache of ARMv7-M Architectures. In *HOST 2015: IEEE International Symposium on Hardware-Oriented Security and Trust*, Washington, United States, May 2015.

References vi

[15] E. Ronen, C. O'Flynn, A. Shamir, and A.-O. Weingarten. Iot goes nuclear: Creating a zigbee chain reaction. Technical report, Weizmann Institute of Science, 2016.

[16] J. M. Schmidt and C. Herbst. A practical fault attack on square and multiply. In *2008 5th Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 53–58, Aug 2008.

[17] B. Yuce, N. F. Ghalaty, H. Santapuri, C. Deshpande, C. Patrick, and P. Schaumont. Software fault resistance is futile: Effective single-glitch attacks. In *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 47–58, Aug 2016.

[18] L. Zussa, J. M. Dutertre, J. Clediere, and B. Robisson. Analysis of the fault injection mechanism related to negative and positive power supply glitches using an on-chip voltmeter. In *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pages 130–135, May 2014.