EM Injection : fault model and locality

S. Ordas[1] , L. Guillaume–Sage[1], P. Maurine[1,2]

[1] LIRMM

[2] CEA-TECH

State of the Art

2002

J.J. Quisquater, D. Samyde :
Eddy current for Magnetic Analysis with Active Sensor

2007

J.-M. Schmidt, M. Hutter :
Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results

2009

A. Alaeldine, T. Ordas, R. Perdriau, P. Maurine, M. Ramdani, L. Torres, M. Drissi
Assessment of the Immunity of Unshielded Multicore Integrated Circuits to Near Field Injection

2011

F. Poucheret, M. Lisart, L. Chusseau, B. Robisson, P. Maurine
Local and Direct EM Injection of Power Into CMOS Integrated Circuits

2012

P. Bayon, L. Bossuet, V. Fischer, F. Poucheret, B. Robisson, P. Maurine
Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator

A. Dehbaoui, J-M. Dutertre, P. Orsatelli, P. Maurine, A. Tria
Injection of transient faults using electromagnetic pulses -Practical results on a cryptographic system

A. Dehbaoui, J-M Dutertre, B. Robisson, A.Tria
Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES

2014

S. Ordas,L. Guillaume-Sage, K. Tobich, J-M. Dutertre, P. Maurine
Evidence of a larger EM-induced fault model

State of the Art

2002 — EM injection allows disrupting the behavior of embedded memories

2007 — J.-M. Schmidt, M. Hutter :
Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results

2009 — A. Alaeldine, T. Ordas, R. Perdriau, P. Maurine, M. Ramdani, L. Torres, M. Drissi
Assessment of the Immunity of Unshielded Multicore Integrated Circuits to Near Field Injection

2011 — F. Poucheret, M. Lisart, L. Chusseau, B. Robisson, P. Maurine
Local and Direct EM Injection of Power Into CMOS Integrated Circuits

2012

P. Bayon, L. Bossuet, V. Fischer, F. Poucheret, B. Robisson, P. Maurine
Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator

A. Dehbaoui, J-M. Dutertre, P. Orsatelli, P. Maurine, A. Tria
Injection of transient faults using electromagnetic pulses -Practical results on a cryptographic system

A. Dehbaoui, J-M Dutertre, B. Robisson, A.Tria
Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES

2014 — S. Ordas,L. Guillaume-Sage, K. Tobich, J-M. Dutertre, P. Maurine
Evidence of a larger EM-induced fault model

State of the Art

2002 — EM injection allows disrupting the behavior of embedded memories

2007 — EM injection allows disrupting the course of a RSA algorithm

2009 — A. Alaeldine, T. Ordas, R. Perdriau, P. Maurine, M. Ramdani, L. Torres, M. Drissi
Assessment of the Immunity of Unshielded Multicore Integrated Circuits to Near Field Injection

2011 — F. Poucheret, M. Lisart, L. Chusseau, B. Robisson, P. Maurine
Local and Direct EM Injection of Power Into CMOS Integrated Circuits

2012

P. Bayon, L. Bossuet, V. Fischer, F. Poucheret, B. Robisson, P. Maurine
Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator

A. Dehbaoui, J-M. Dutertre, P. Orsatelli, P. Maurine, A. Tria
Injection of transient faults using electromagnetic pulses -Practical results on a cryptographic system

A. Dehbaoui, J-M Dutertre, B. Robisson, A.Tria
Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES

2014 — S. Ordas,L. Guillaume-Sage, K. Tobich, J-M. Dutertre, P. Maurine
Evidence of a larger EM-induced fault model

State of the Art

2002 — EM injection allows disrupting the behavior of embedded memories

2007 — EM injection allows disrupting the course of a RSA algorithm

2009 — Harmonic EM Injection modifies the **propagation delays** of logical paths

2011

F. Poucheret, M. Lisart, L. Chusseau, B. Robisson, P. Maurine
Local and Direct EM Injection of Power Into CMOS Integrated Circuits

2012

P. Bayon, L. Bossuet, V. Fischer, F. Poucheret, B. Robisson, P. Maurine
Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator

A. Dehbaoui, J-M. Dutertre, P. Orsatelli, P. Maurine, A. Tria
Injection of transient faults using electromagnetic pulses -Practical results on a cryptographic system

A. Dehbaoui, J-M Dutertre, B. Robisson, A.Tria
Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES

2014

S. Ordas,L. Guillaume-Sage, K. Tobich, J-M. Dutertre, P. Maurine
Evidence of a larger EM-induced fault model

State of the Art

2002 — EM injection allows disrupting the behavior of embedded memories

2007 — EM injection allows disrupting the course of a RSA algorithm

2009 — Harmonic EM Injection modifies the **propagation delays** of logical paths

2011 — Harmonic EM Injection modifies **the oscillating Frequency** of an internal clock generator

2012

P. Bayon, L. Bossuet, V. Fischer, F. Poucheret, B. Robisson, P. Maurine
Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator

A. Dehbaoui, J-M. Dutertre, P. Orsatelli, P. Maurine, A. Tria
Injection of transient faults using electromagnetic pulses -Practical results on a cryptographic system

A. Dehbaoui, J-M Dutertre, B. Robisson, A.Tria
Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES

2014

S. Ordas,L. Guillaume-Sage, K. Tobich, J-M. Dutertre, P. Maurine
Evidence of a larger EM-induced fault model

State of the Art

2002 — EM injection allows disrupting the behavior of embedded memories

2007 — EM injection allows disrupting the course of a RSA algorithm

2009 — Harmonic EM Injection modifies the **propagation delays** of logical paths

2011 — Harmonic EM Injection modifies **the oscillating Frequency** of an internal clock generator

2012 — Harmonic EM Injection modifies the behavior or RO based TRNG **(phase locking)**

A. Dehbaoui, J-M. Dutertre, P. Orsatelli, P. Maurine, A. Tria
Injection of transient faults using electromagnetic pulses -Practical results on a cryptographic system

A. Dehbaoui, J-M Dutertre, B. Robisson, A.Tria
Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES

2014 — S. Ordas,L. Guillaume-Sage, K. Tobich, J-M. Dutertre, P. Maurine
Evidence of a larger EM-induced fault model

State of the Art

2002 — EM injection allows disrupting the behavior of embedded memories

2007 — EM injection allows disrupting the course of a RSA algorithm

2009 — Harmonic EM Injection modifies the **propagation delays** of logical paths

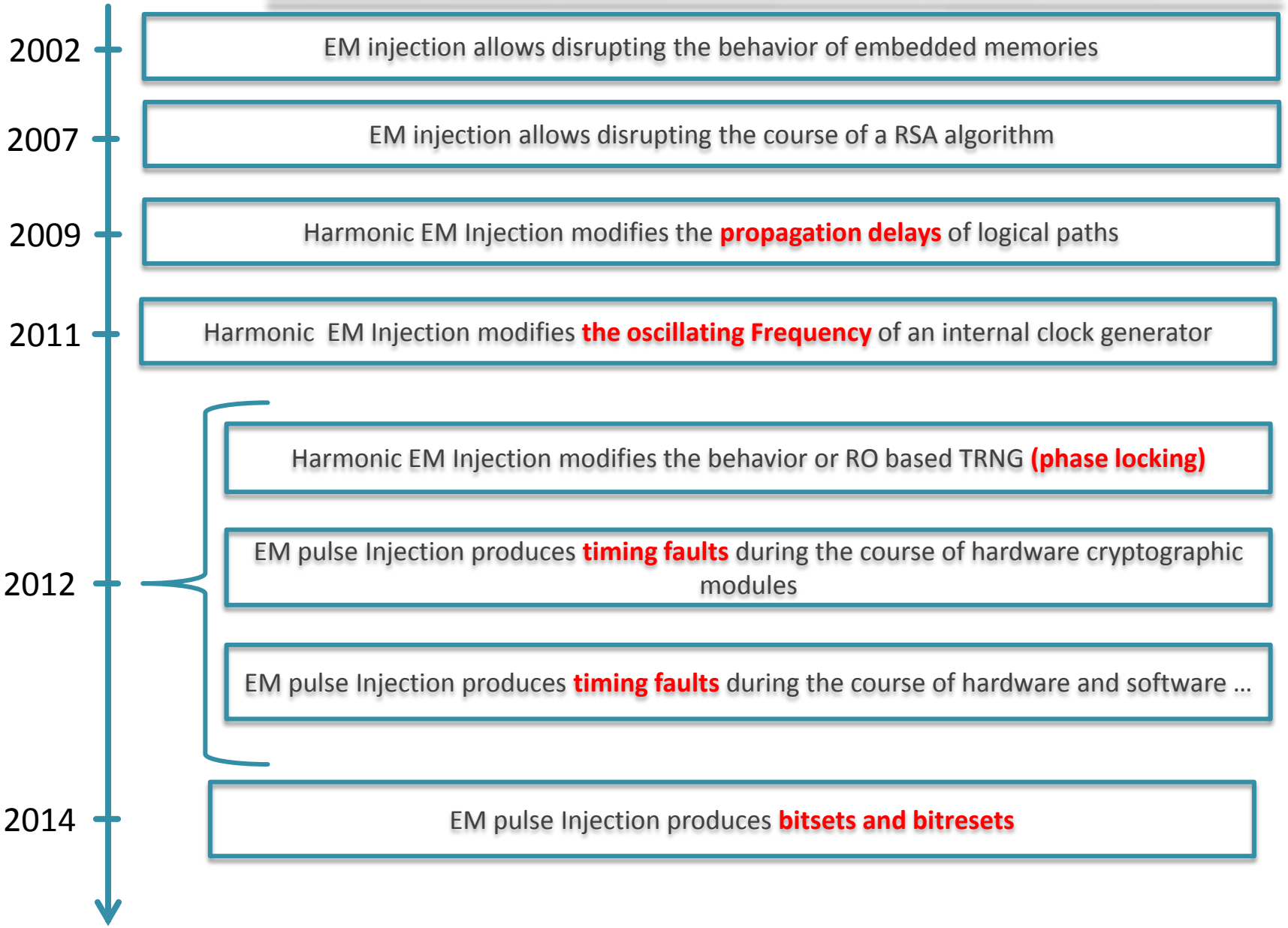
2011 — Harmonic EM Injection modifies **the oscillating Frequency** of an internal clock generator

2012

- Harmonic EM Injection modifies the behavior or RO based TRNG **(phase locking)**
- EM pulse Injection produces **timing faults** during the course of hardware cryptographic modules
- EM pulse Injection produces **timing faults** during the course of hardware and software …

2014 — S. Ordas,L. Guillaume-Sage, K. Tobich, J-M. Dutertre, P. Maurine
Evidence of a larger EM-induced fault model

State of the Art

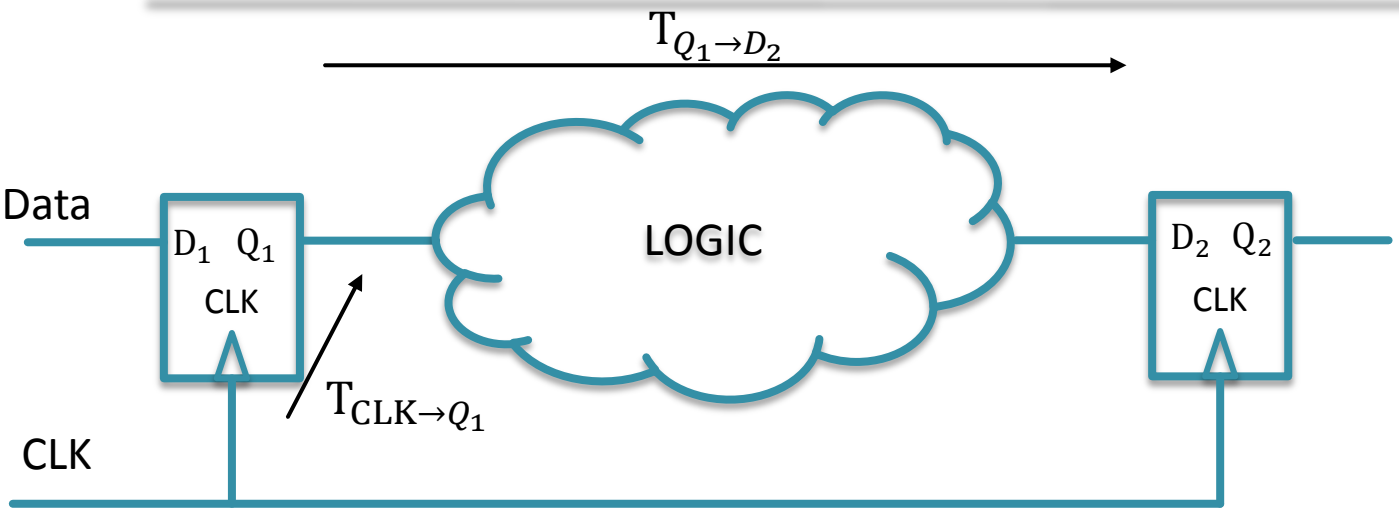


CONCLUSION OF OUR PREVIOUS PAPER

1. Polarity of EM injection is important
2. EM injection has a local effect
3. EM injection induce bitsets and bitresets
4. Pulse must have a high voltage to produce bitset and bitreset

What kind of faults appears on an operating circuit?

TIMING FAULTS MODEL

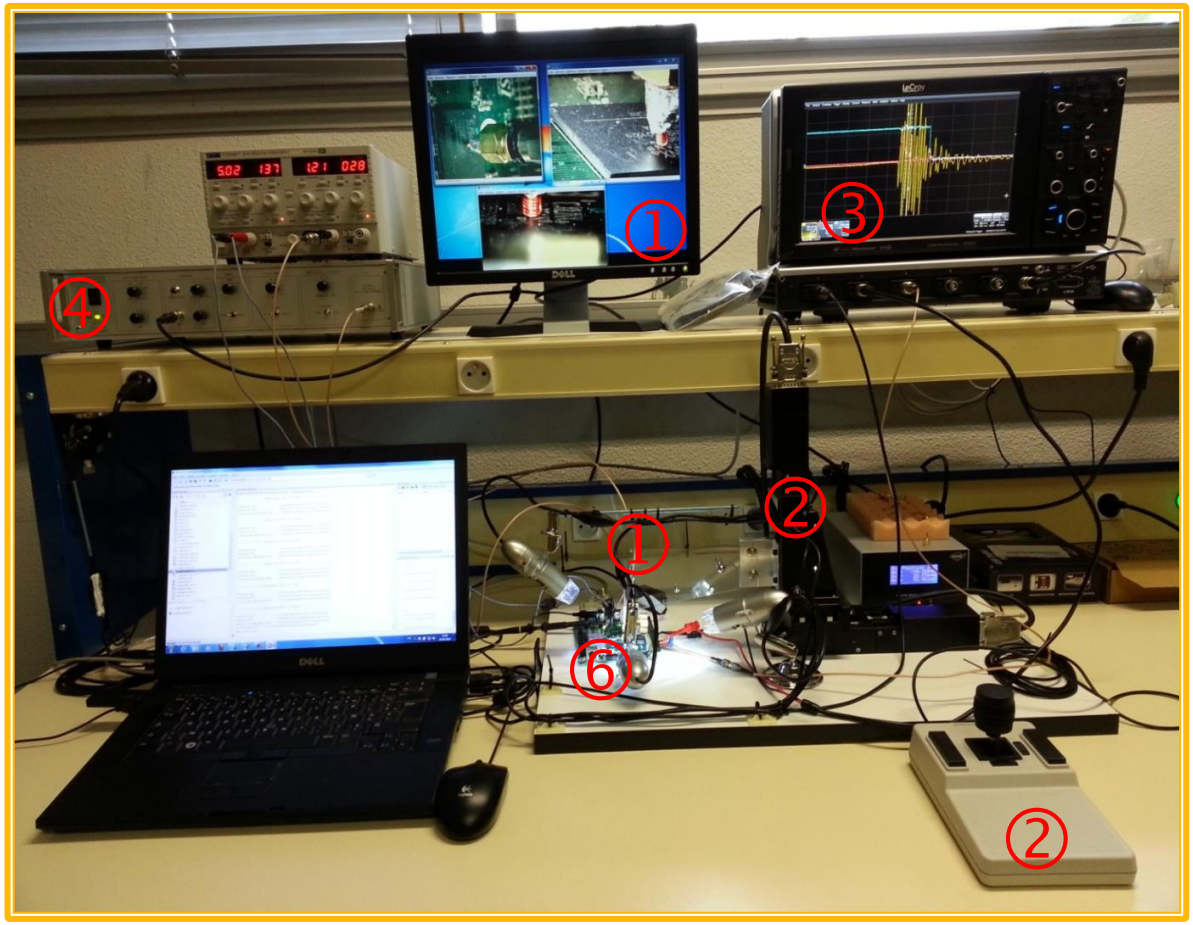


Timing constraint :

$$T_{CLK \rightarrow Q_1} + T_{Q_1 \rightarrow D_2} < T_{CLK} - T_{skew} - T_{Setup}$$

EM Injection induces Setup time constraint violations

EM Injection Platform: overview



① 3-axes vision system

② 3-axes positioning system

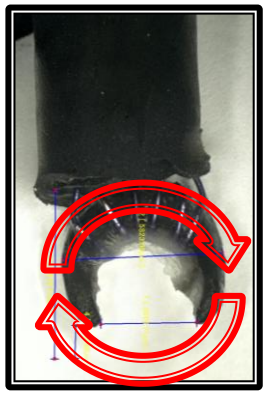
③ Oscilloscope

④ Pulse generator

⑥ Hand made injection probes

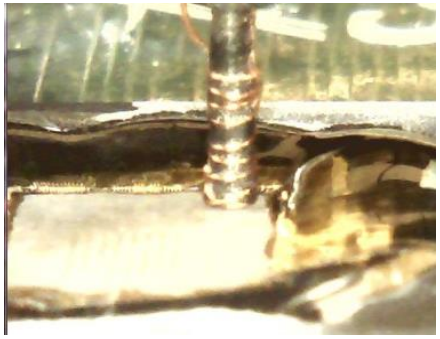
⑦ a laptop

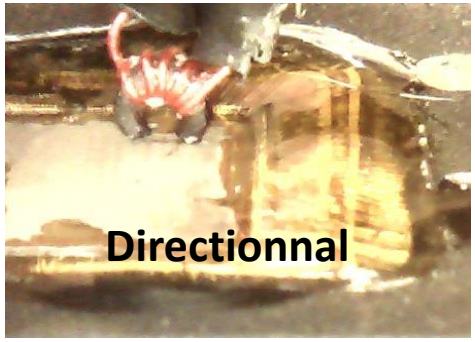
HAND MADE INJECTION PROBES



Magnetic flux is spread over a large surface

Concentrate the magnetic flux on a reduced area of the IC surface using concentric field lines

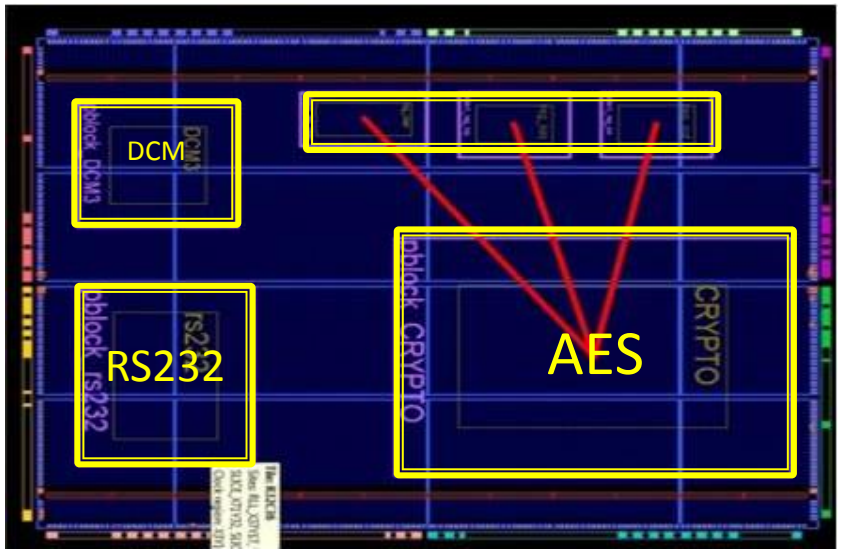




EXPERIMENTATION ON AN OPERATING CIRCUIT

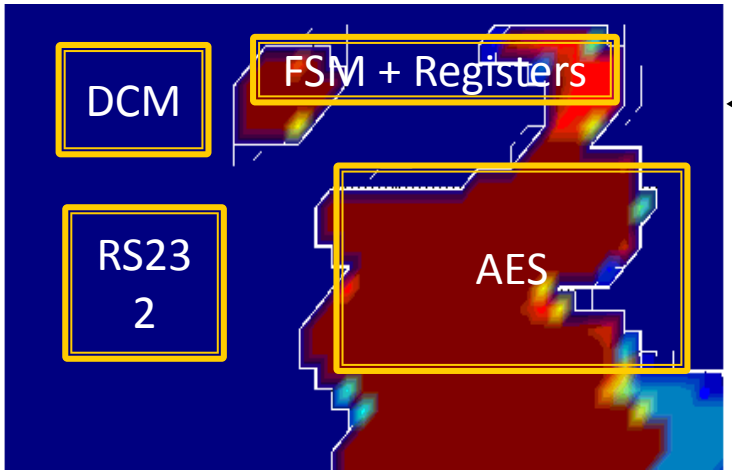
To evaluate if some areas of the system are more sensitive to EM pulsed than others

- Fpga Xilinx Spartan 3
- Vdd= 1.2V
- Frequency : 100MHz (generated by DCM)
- Cartography step : 200µm
- Vpulse = 44V << 110V
- Hand made probe
- 100 shoots per position

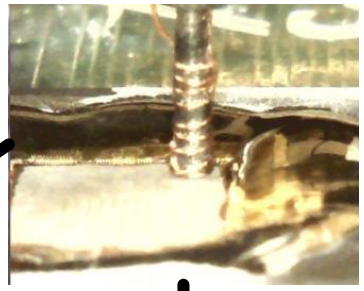


LOCALITY OF THE EM INJECTION

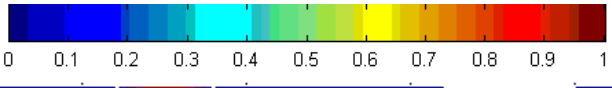
bad ciphering

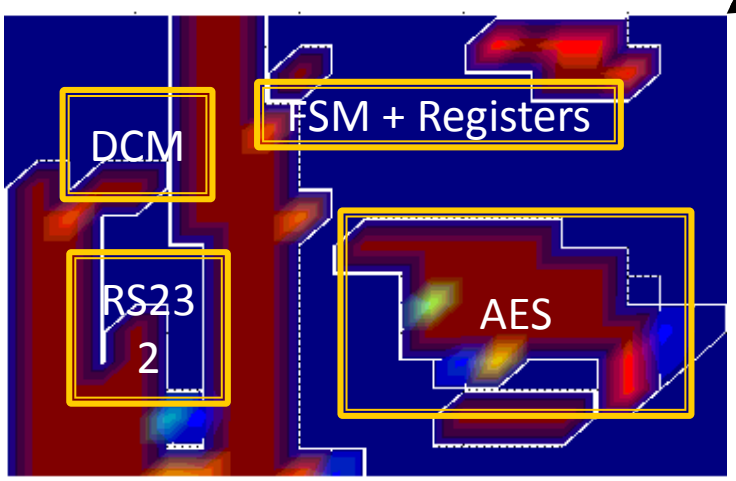


Crescent injector

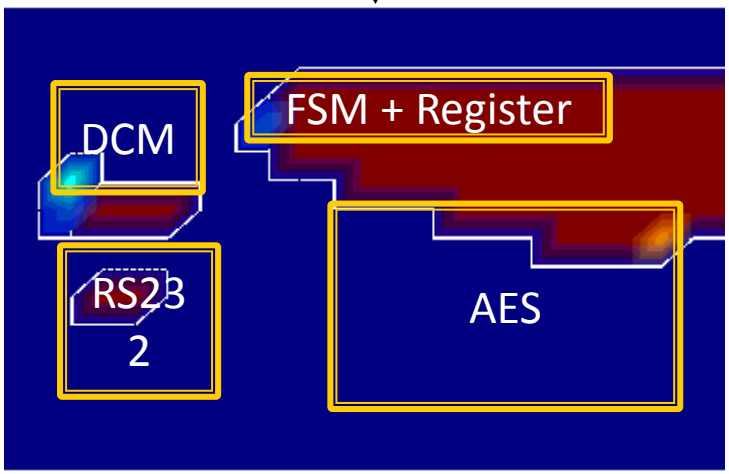


flathead injector



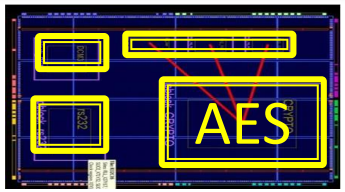


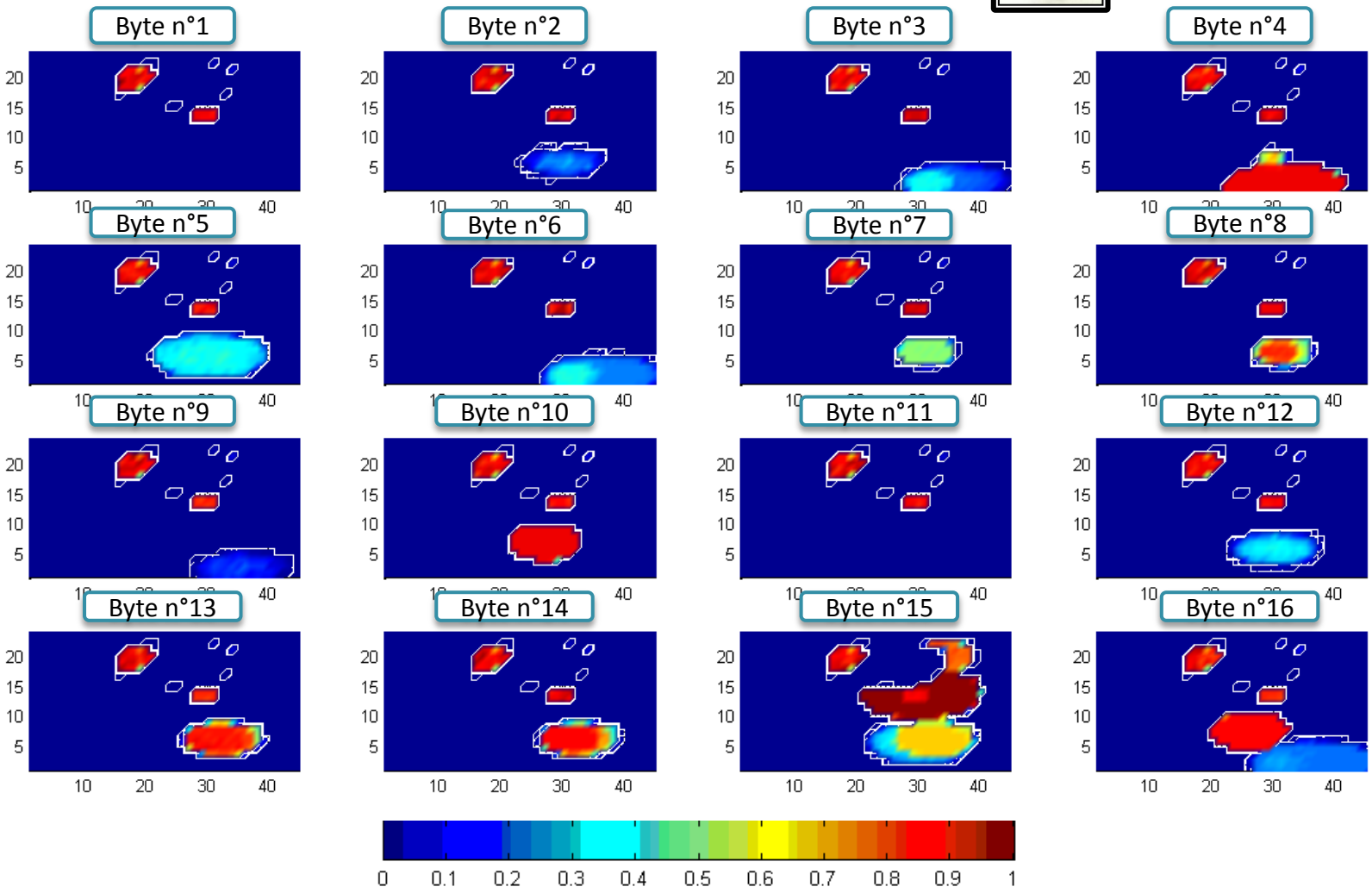
bad ciphering



no-response

LOCALITY OF EACH BYTE FAULTED

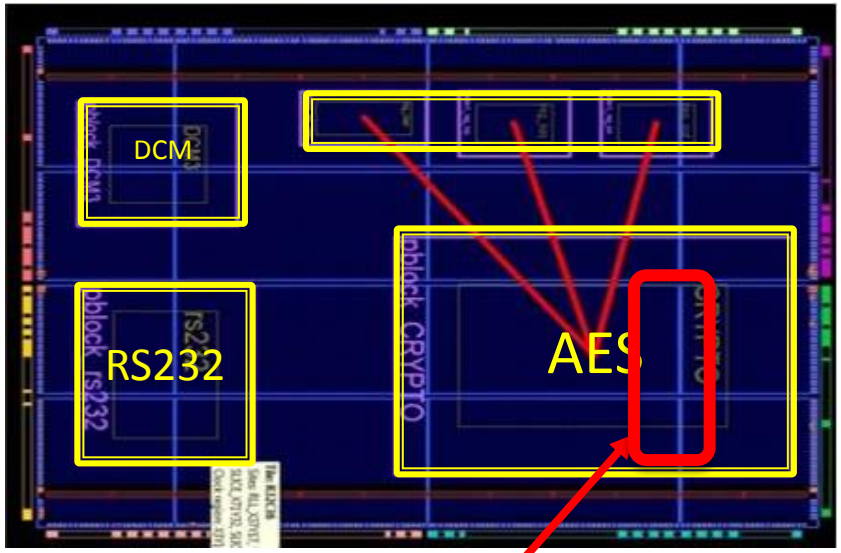




EXPERIMENTATION ON AN OPERATING CIRCUIT

To evaluate if some moments of the AES calculus are more sensitive to EM pulsed than others

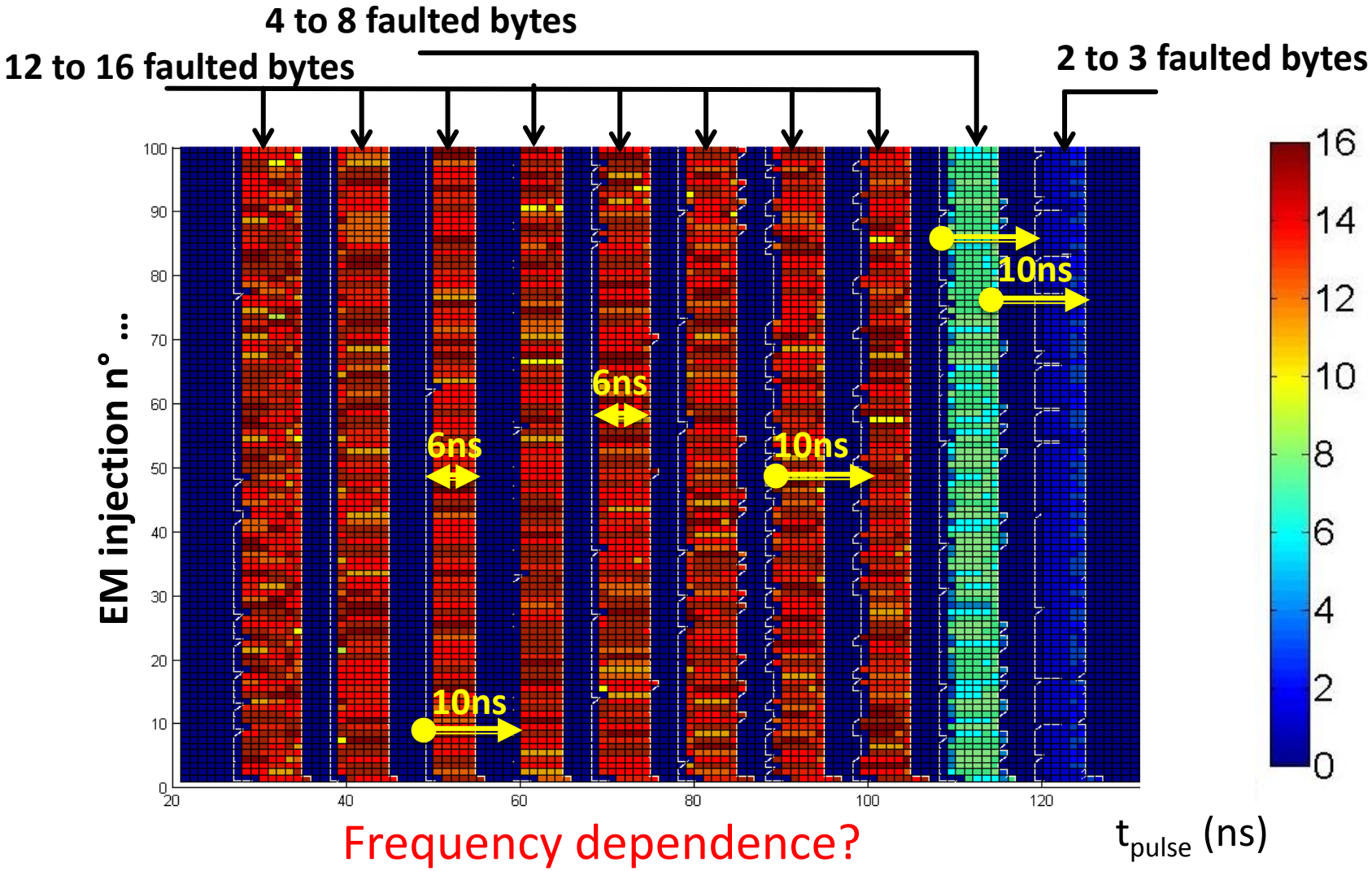
- Fpga Xilinx Spartan 3
- Vdd= 1,2V
- Frequency : 100MHz (generated by DCM)
- Vpulse = 44V << 110V
- Hand made probe



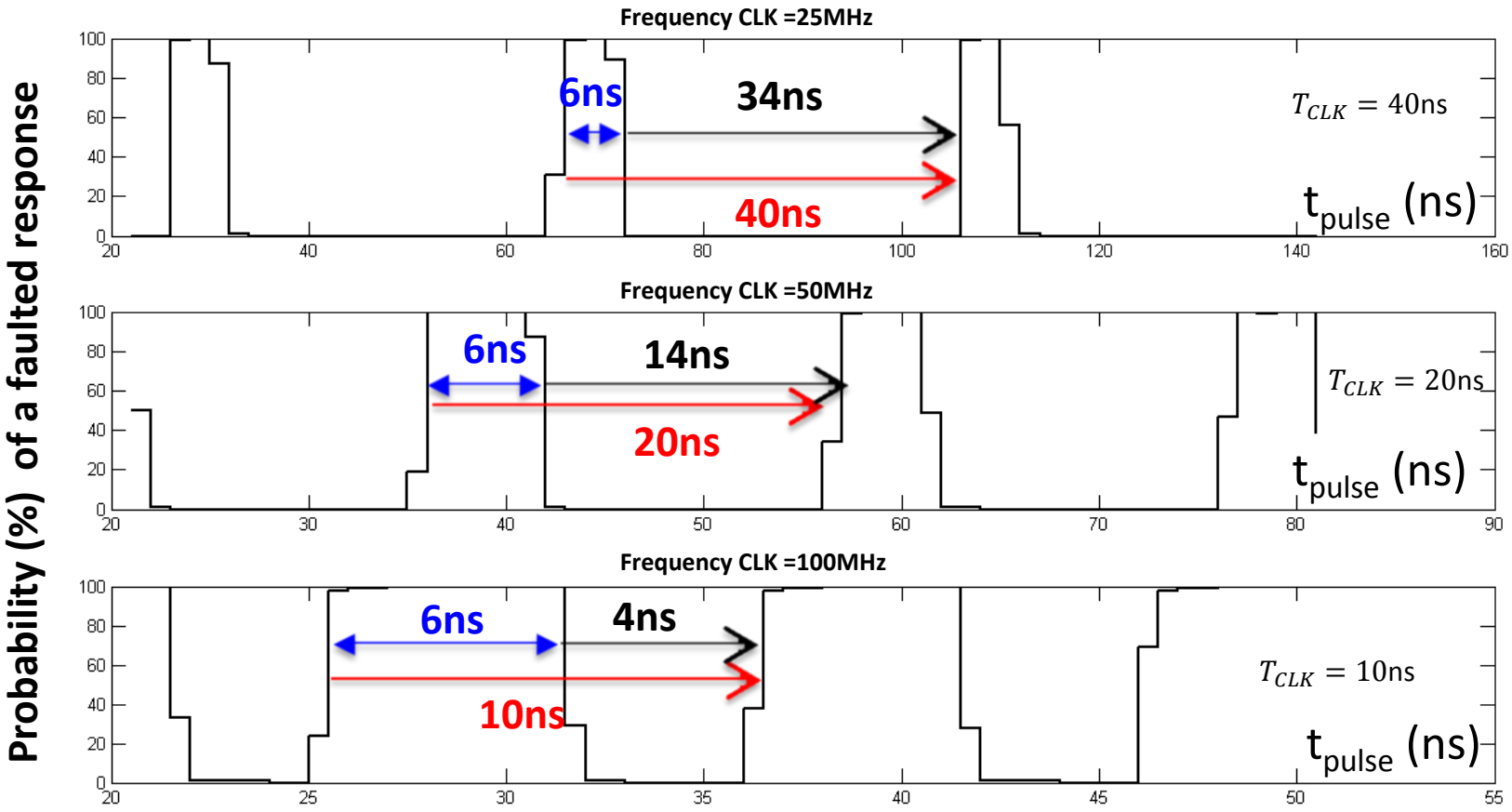
- Moment of the injection varies for covering all the ciphering

LOCALIZATION IN TIME OF THE FAULTS

$F_{CLK} = 100MHz \quad T_{CLK} = 10\text{ns}$



FREQUENCY DEPENDENCE?

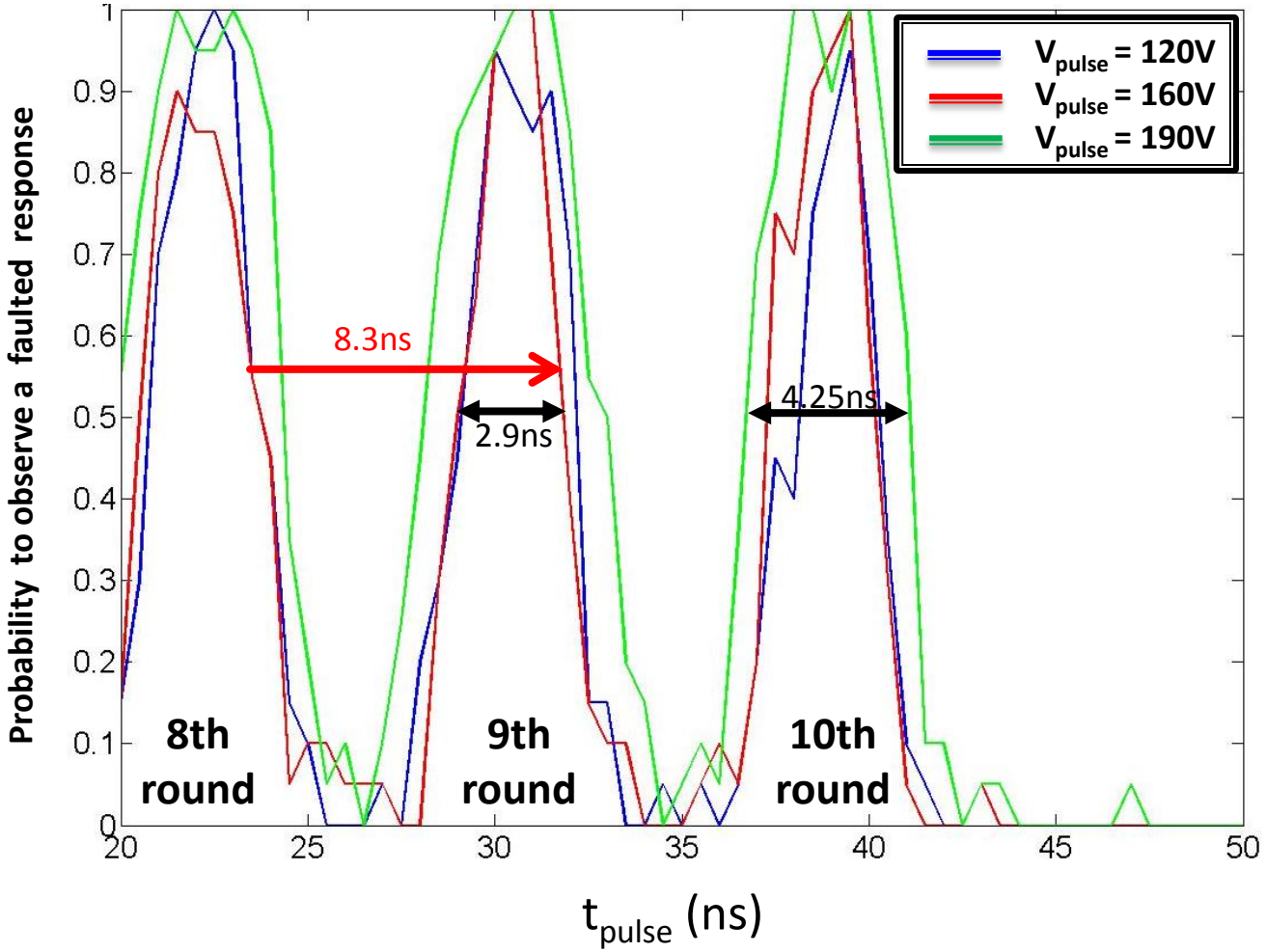


No frequency dependence

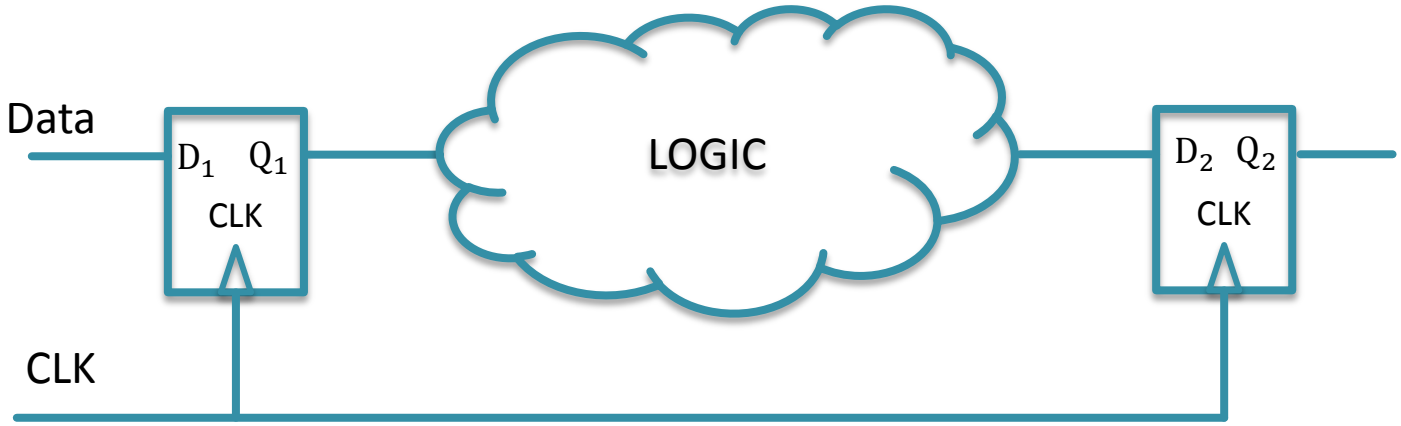
Faults are not timing faults

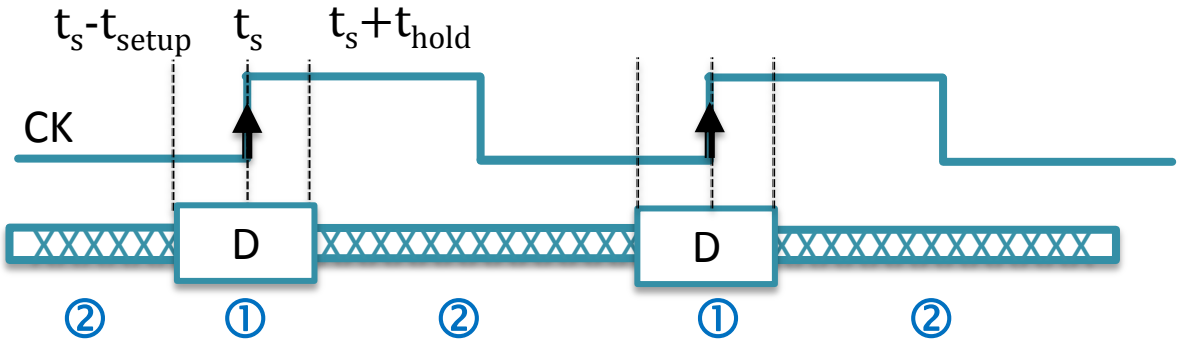
EXPERIMENT VALIDATION ON MICRO-CONTROLLER

- Experiment realized on an AES hardware
- Frequency of the CLK : 120MHz



OPERATING CIRCUIT



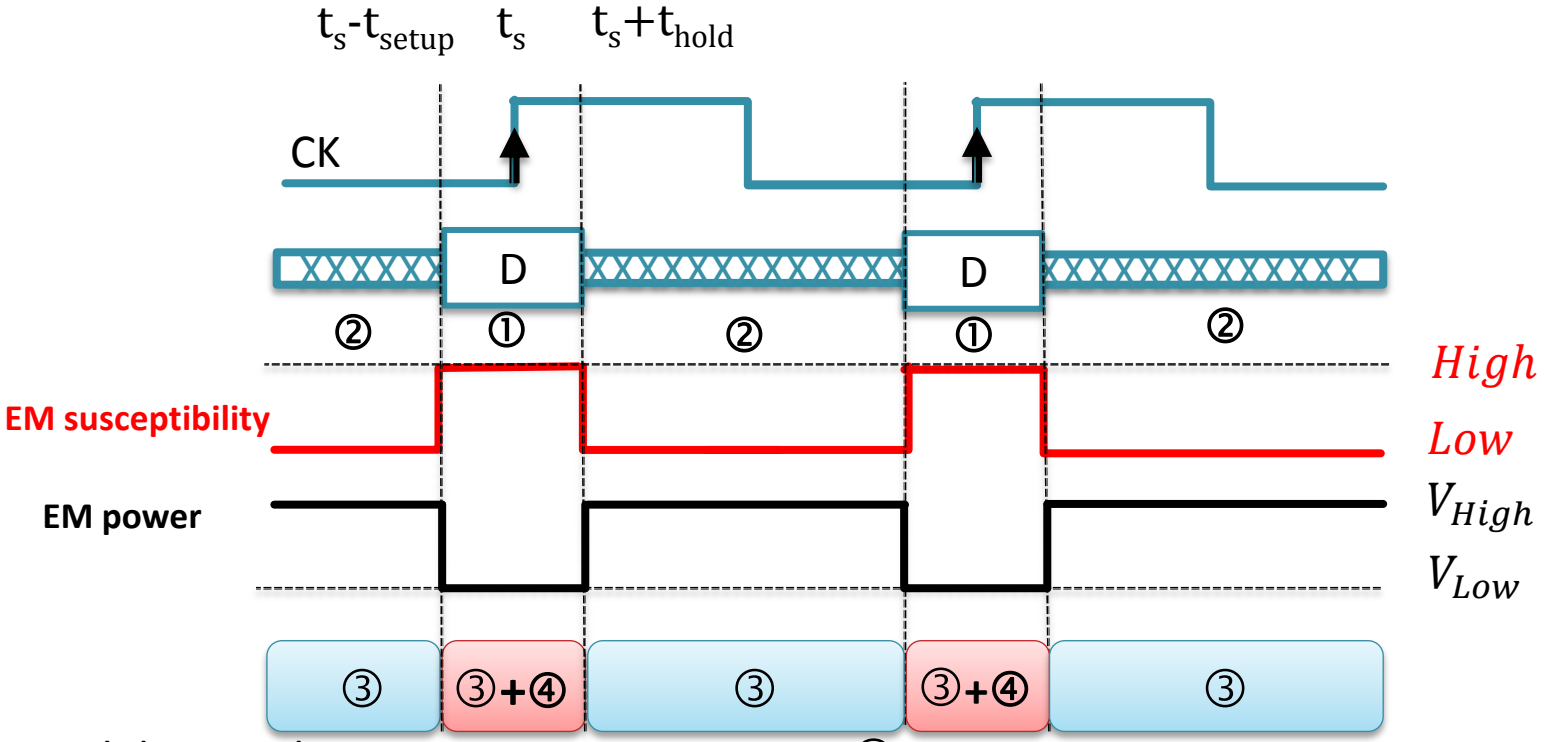


① : Stability window

② : Processing window

FAULT MODEL

- Sampling faults
  - Disrupt an input signal of the DFF (CLK, Data ,Reset, Set)
  - Disrupt during the stability window (t_{setup}+t_{hold} around rising clock edges)



① : Stability window

② : Processing window

③ : Bitset or bitreset produced

④ : Sampling fault produced

CONCLUSION

1. EM injection has a local effect
2. EM injection may induces bitsets and bitresets
3. EM injection do not produce timing faults
4. EM injection easily disrupts the switching of DFF
5. Define a fault model for EM Injection (the sampling fault model)

Thank you for your attention

Questions?