Pré-GDR Sécurité Informatique

Journées Nationales 2018
Pré-GDR Sécurité Informatique
Sécurité des systèmes matériels

Hardware attacks: theory and experimental state-of-the-art of laser fault injection attacks

Jean-Max Dutertre, 30 mai 2018, Jussieu

Département Systèmes et Architectures Sécurisées
Mines Saint-Etienne, Centre de Microélectronique de Provence
13541 Gardanne FRANCE

MINES Saint-Étienne
Une école de l'IMT

Institut Mines-Télécom

❑ Laser fault injection?

1997 Boneh et al. introduced **fault** attacks

Hardware attack of crypto./secure devices

2002 Skorobogatov et al. introduced **laser** fault inject.

Secure devices: CMOS 350 nm

One single transistor under a laser beam (1 µm)

2018 Continuous CMOS tech. shrinkage

Secure devices: CMOS 40 nm

One logic gate under a laser beam (1 µm)

❑ Laser fault injection?

1965 Habing introduced laser emulation of SEE

Emulation of radiation induced Single Event Effects

1997 Boneh et al. introduced **fault** attacks

Hardware attack of crypto./secure devices

2002 Skorobogatov et al. introduced **laser** fault inject.

Secure devices: CMOS 350 nm

One single transistor under a laser beam (1 µm)

2018 Continuous CMOS tech. shrinkage

Secure devices: CMOS 40 nm

One logic gate under a laser beam (1 µm)

! Radiation community: best and largest bibliography on laser-Si interaction

Position of the problem

❑ Laser fault injection?

- Pulsed lasers are used to inject faults into running secure devices for the purpose of retrieving secret information.

❑ Why does it matters?

- An efficient fault injection tool
- An accurate fault injection tool
- Part of security certification processes

Agenda

I. Introduction

Hardware attacks

II. Theory of laser fault injection

Physics and basics of laser fault injection

Fault models of laser injection

III. Practice of laser fault injection

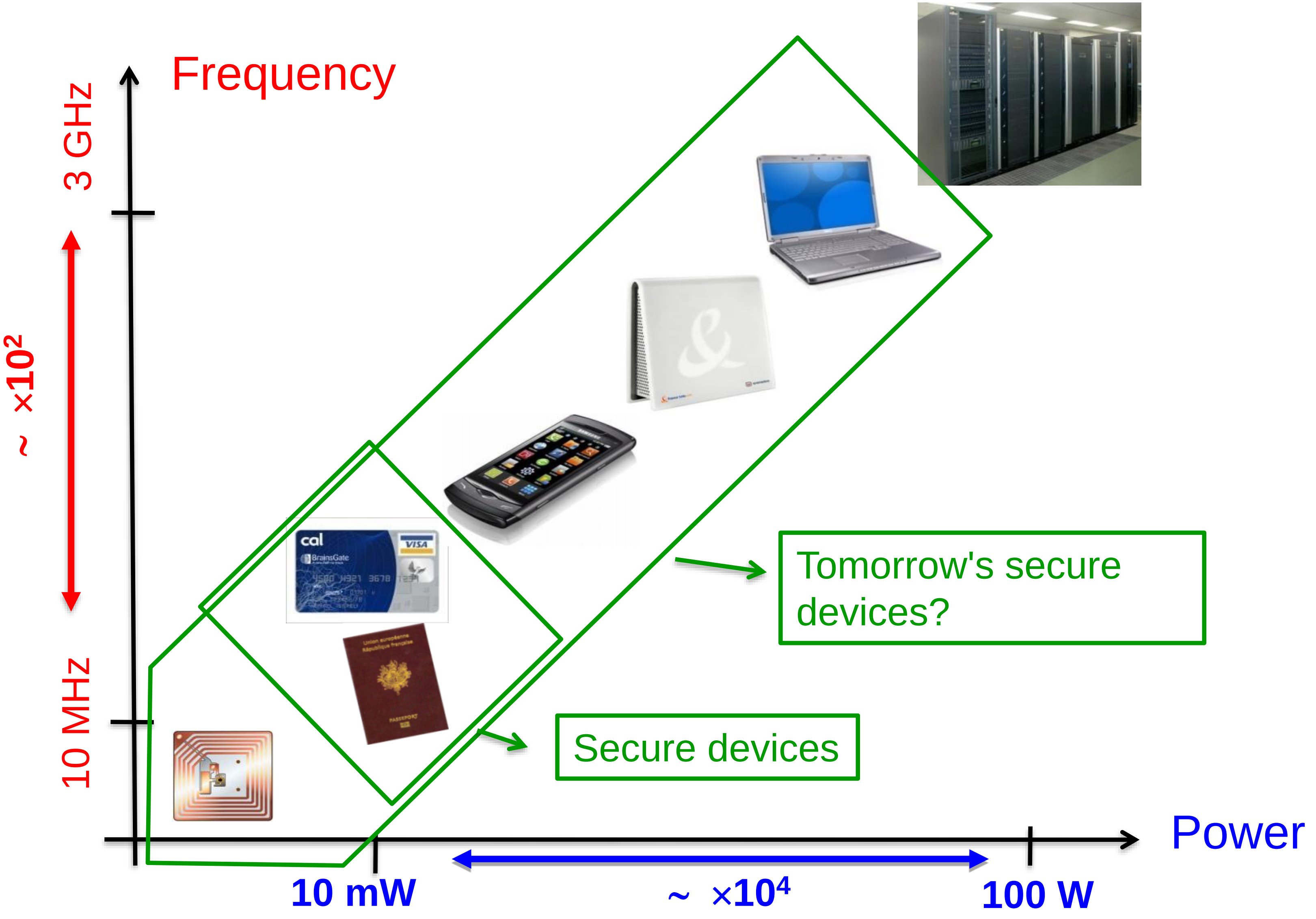
Laser fault injection bench

Questions raised by technological advances

Experiment results (from CMOS 350 nm to 28 nm)

IV. Conclusion

❑ Secure devices



❑ Secure devices

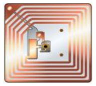
- Applications:
  - Identification,

  - Smartcards, banking,

  - Pay TV,

  - Smartphone,

  - etc.



Pocket/mobile objects

⇩

Vulnerabilities
(lost, theft, etc.)

- Security features:
  - PIN code / password => user identification,
  - Cryptography => secure communications

❑ Secure devices

- Cryptography provides:
  - confidentiality,
  - authentication,
  - integrity,
  - non-repudiation.

- Cryptography: mathematically secure

  Unbreakable given math. knowledge and computation capacities

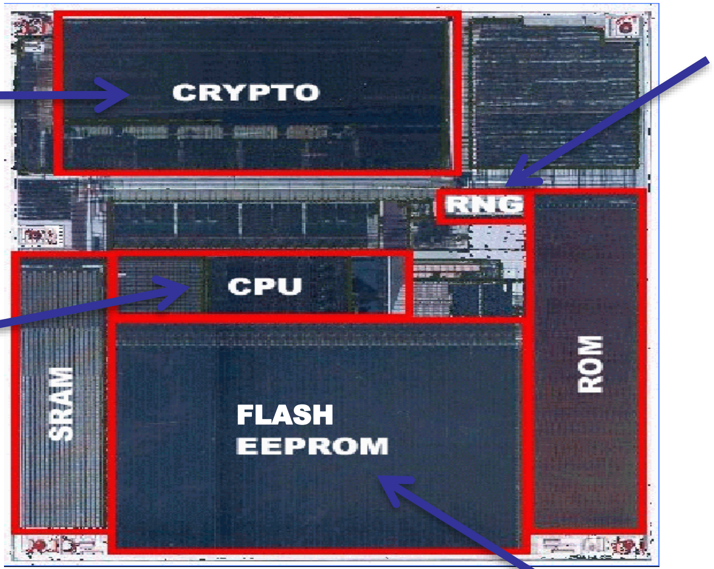
Beware hardware/physical implementation

⇨ **Physical/hardware attacks**

- Hardware attacks’ target: secure devices

Crypto:
Crypto accelerator

CPU:
Software cryptography



RNG: random number generator
Key generation

Flash/EEPROM:
non-volatile memory
Store secrets, private data
and KEYS !

Hardware implementation of security and crypto. primitives gave birth to hardware attacks (as opposed to software attacks)

❑ Hardware attacks

- **Goal:** retrieve secret information or encryption keys, PIN bypass, gain unauthorized access, etc.

- Observation attacks: passive attacks
  - encryption time,
  - power consumption (which correlates with the handled data),
  - EM emissions (which correlates with the handled data),
  - photon emission, etc.

Observation/eavesdropping of a physical parameter that is correlated to the data handled by the target circuit.

I. Introduction

- Perturbation attacks / fault attacks: active attacks

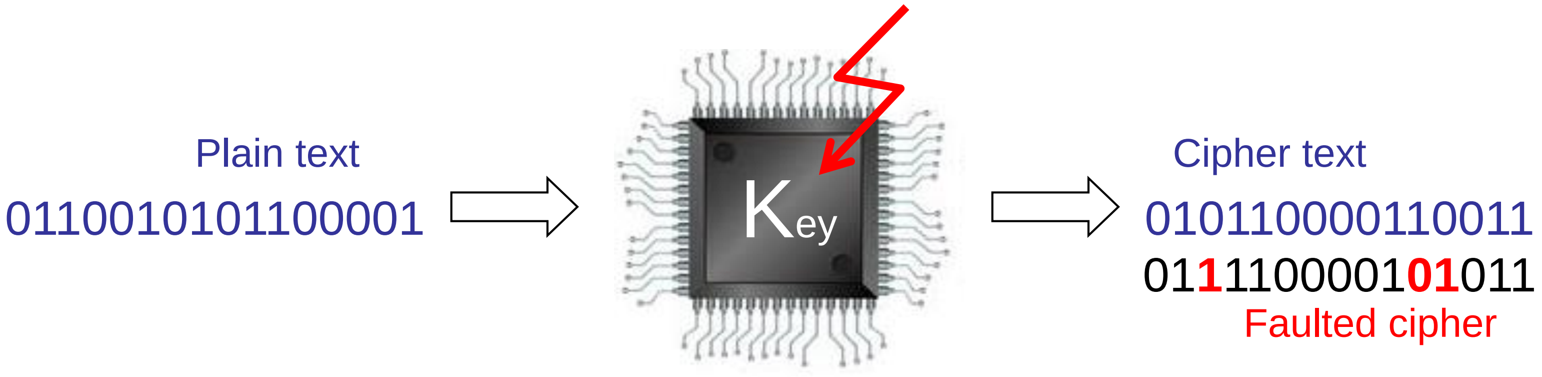
Disturbing the target’s nominal operating conditions in order to induce an abnormal behavior (on a running and functional device)

- Software modification

  instruction skip (e.g. PIN bypass)

- Fault injection

  inducing an information leakage to retrieve encryption keys (differential fault attack, DFA)



A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache: Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures, proceedings of the IEEE, 100:3056 – 3076, 2012.

- Requirements of the fault injection process?

  Strong → **fault model**:

  - location (e.g. round calculations or key expansion),
  - injection time (regarding the course of the algorithm),
  - **nb. of faulted bits/bytes**

⇨ Single-bit / single-byte fault models associated with very efficient DFA schemes

The attacker needs a fine control on the fault injection process

C. Giraud: DFA on AES, Lecture Notes in Computer Science, 2005, Springer Berlin / Heidelberg, Volume 3373

G. Piret, J.-J. Quisquater: A Differential Fault Attack Technique Against SPN Structures, with Application to the AES, CHES 2003, LNCS 2779, Springer-Verlag

- Fault injection techniques

	Control on			reproducibility	cost	ease of use
	injection time	localization	# faulted bits			
Clock glitch (digital)	very good	low	very good	good	low	very good
Power glitch (analog)	good	low	very good	good	average	good
Overclocking Underpowering Temperature	low	low	good	good	low	good
EM pertubation	good	average	very good	good	average	good
Laser	good	very good	very good	good	high	good

- Laser fault injection

Why considering this costly FI technique?

- An efficient fault injection tool
  - radioactive effects emulation (1965, D. Habing),
  - 1st publication related to secure devices in 2002 (S. Skorobogatov).
- An accurate fault injection tool
  - location / timing / focalization (nb. of faulted bits).
- Security certification (common criteria/EAL)
  - part of the certification process of secure devices,
  - high level of certification mandatory to access secure devices market

S. P. Skorobogatov and R. J. Anderson: Optical fault induction attacks, CHES 2002.

D. Habing: The use of lasers to simulate radiation-induced transients in semiconductor devices and circuits. Nuclear Science, IEEE Transactions on, 12(5):91–100, Oct 1965.

Agenda

I. Introduction

Hardware attacks

II. Theory of laser fault injection

Physics and basics of laser fault injection

Fault models of laser injection

III. Practice of laser fault injection

Laser fault injection bench

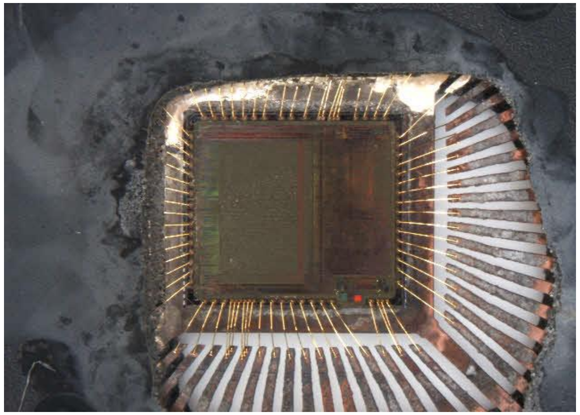
Questions raised by technological advances

Experiment results (from CMOS 350 nm to 28 nm)

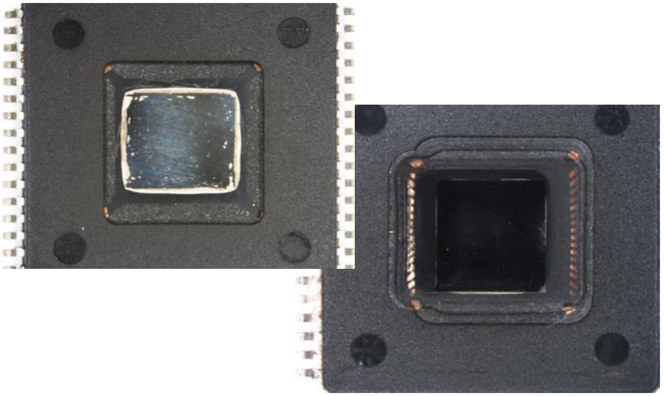
IV. Conclusion

❑ Physics of laser fault injection

- Laser beam: semi invasive (package mechanical/chemical opening)

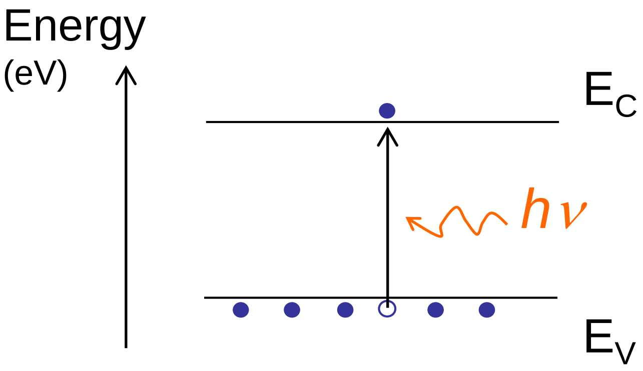


Front side



Backside

- laser – silicon interaction: the photoelectric effect

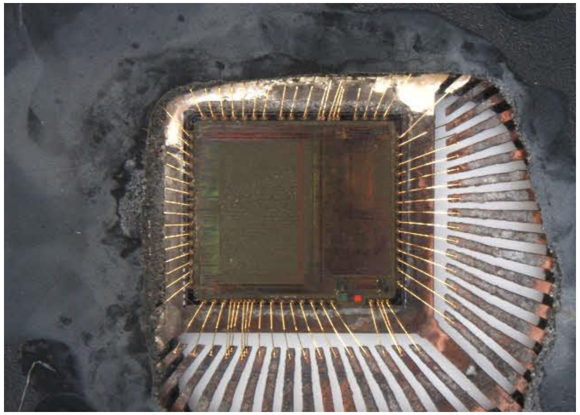


$$h\nu > E_g$$

$$\boxed{\lambda_{laser} < 1{,}1\ \mu m}$$

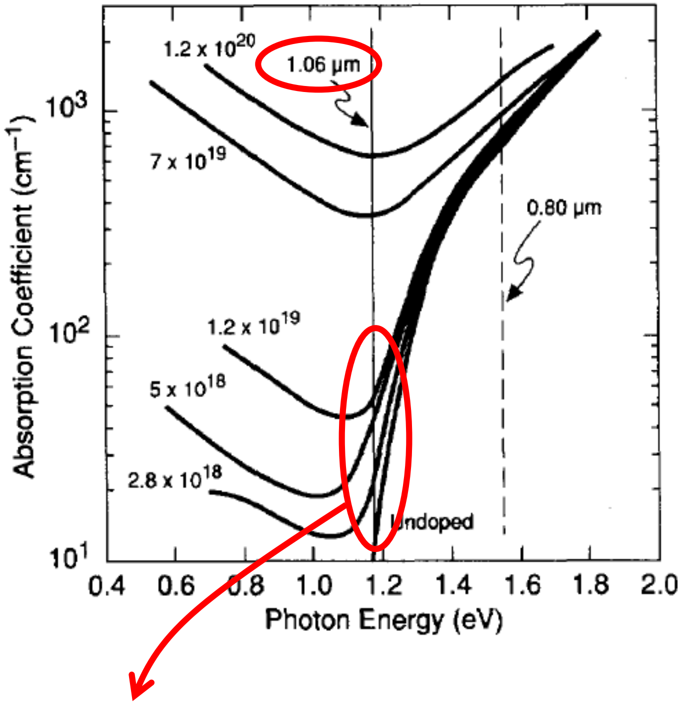
❑ Physics of laser fault injection

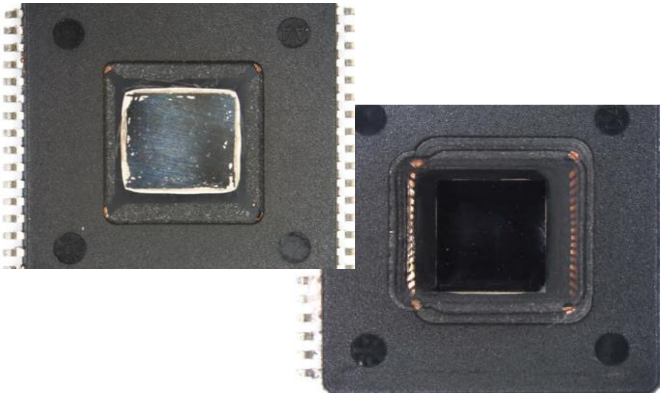
- Laser beam: semi invasive (package mechanical/chemical opening)



Front side

- Front side: reflection on metal paths (e.g. 532nm, green)





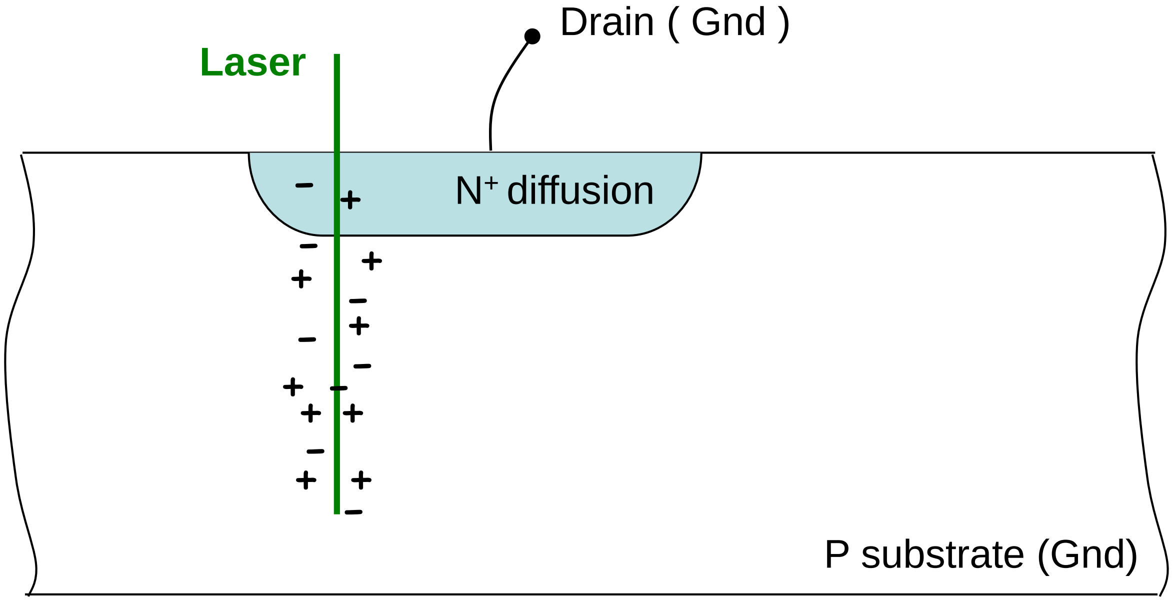
Backside

- Backside: λ = infrared (e.g. 1064nm) (die thinning)

II. Theory of laser fault injection

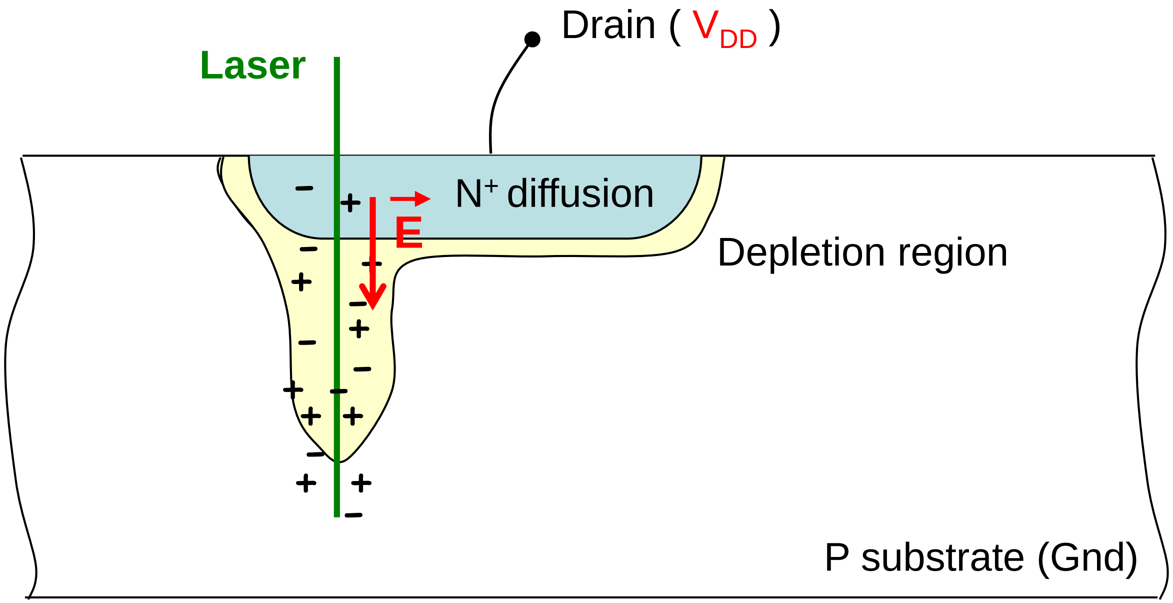
- Photoelectric effect:

  from a laser pulse to transient current generation



- Photoelectric effect:

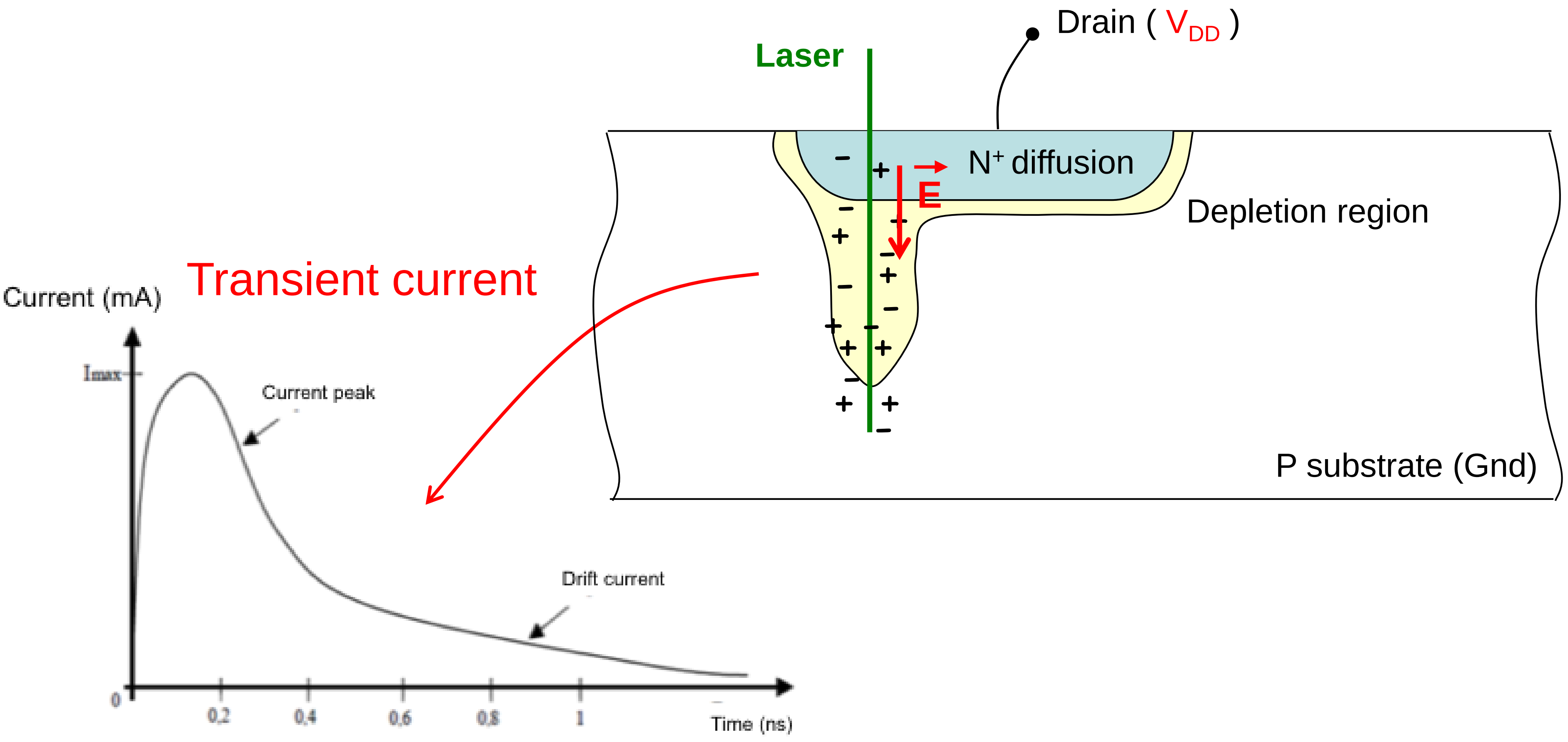
  from a laser pulse to transient current generation



II. Theory of laser fault injection

- Photoelectric effect:

  from a laser pulse to transient current generation



Laser

Drain (V_{DD})

N^+ diffusion

E

Depletion region

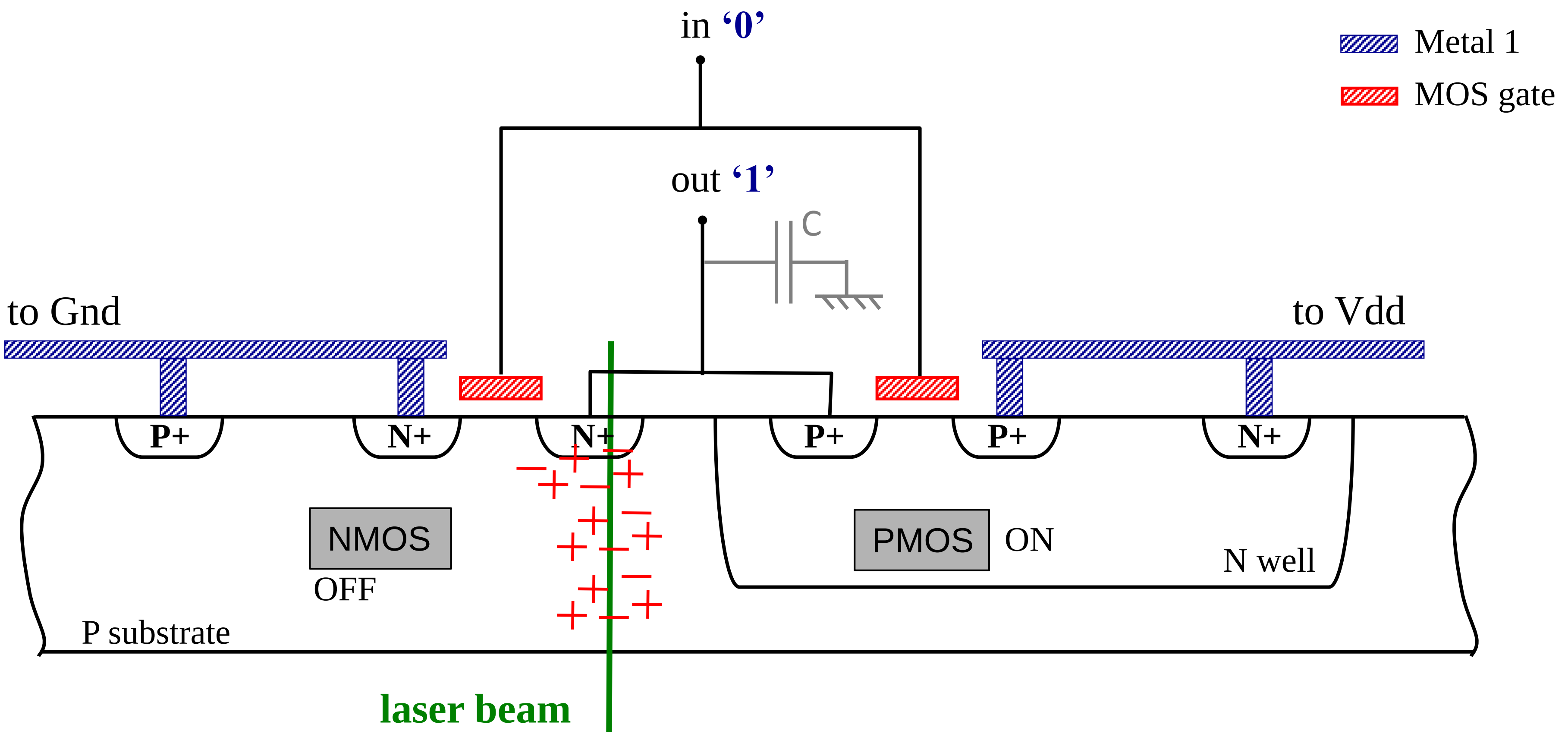
P substrate (Gnd)

Transient current

⇨ Laser sensitive areas: reverse biased PN junctions

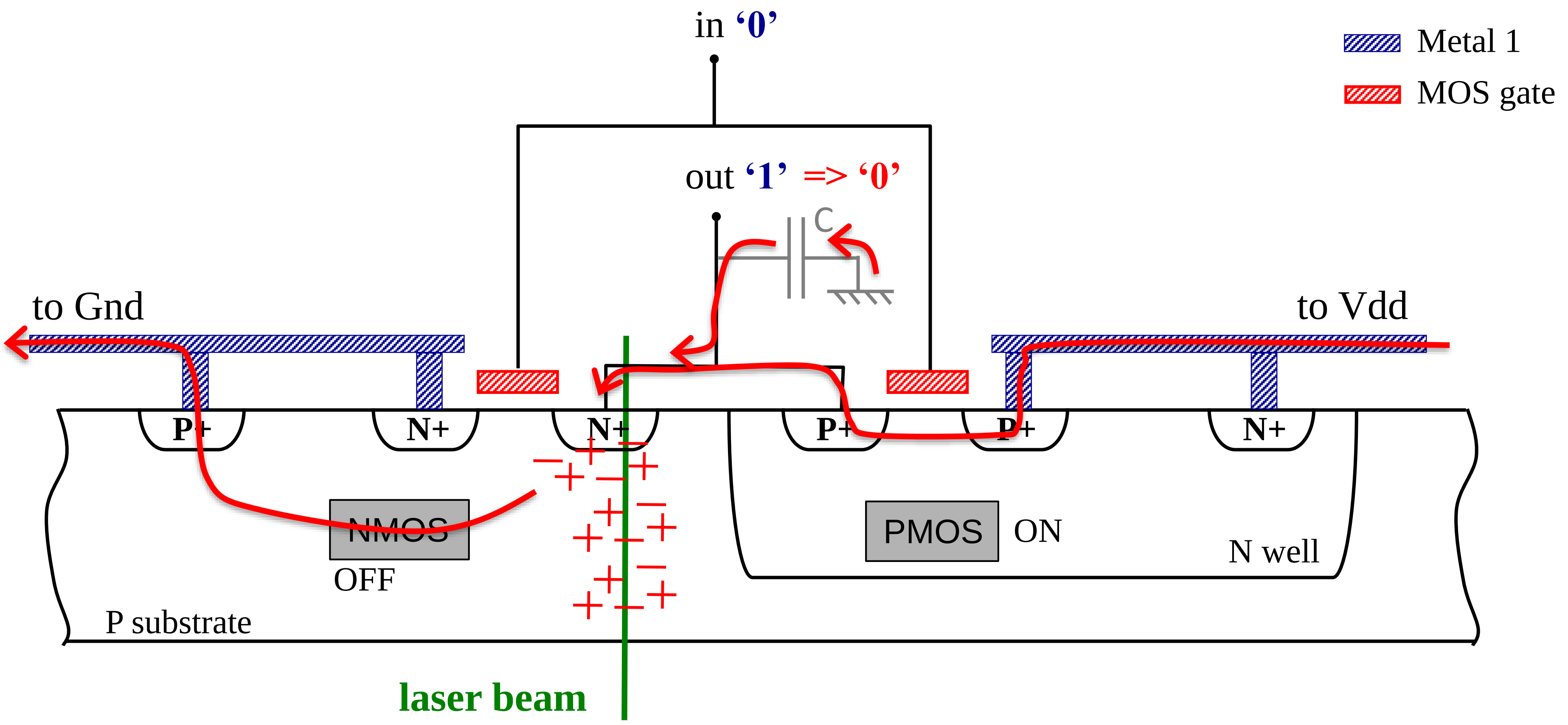
- Fault injection mechanism (the inverter case)

  from a transient current to a voltage transient (a.k.a. SET, single event transient)



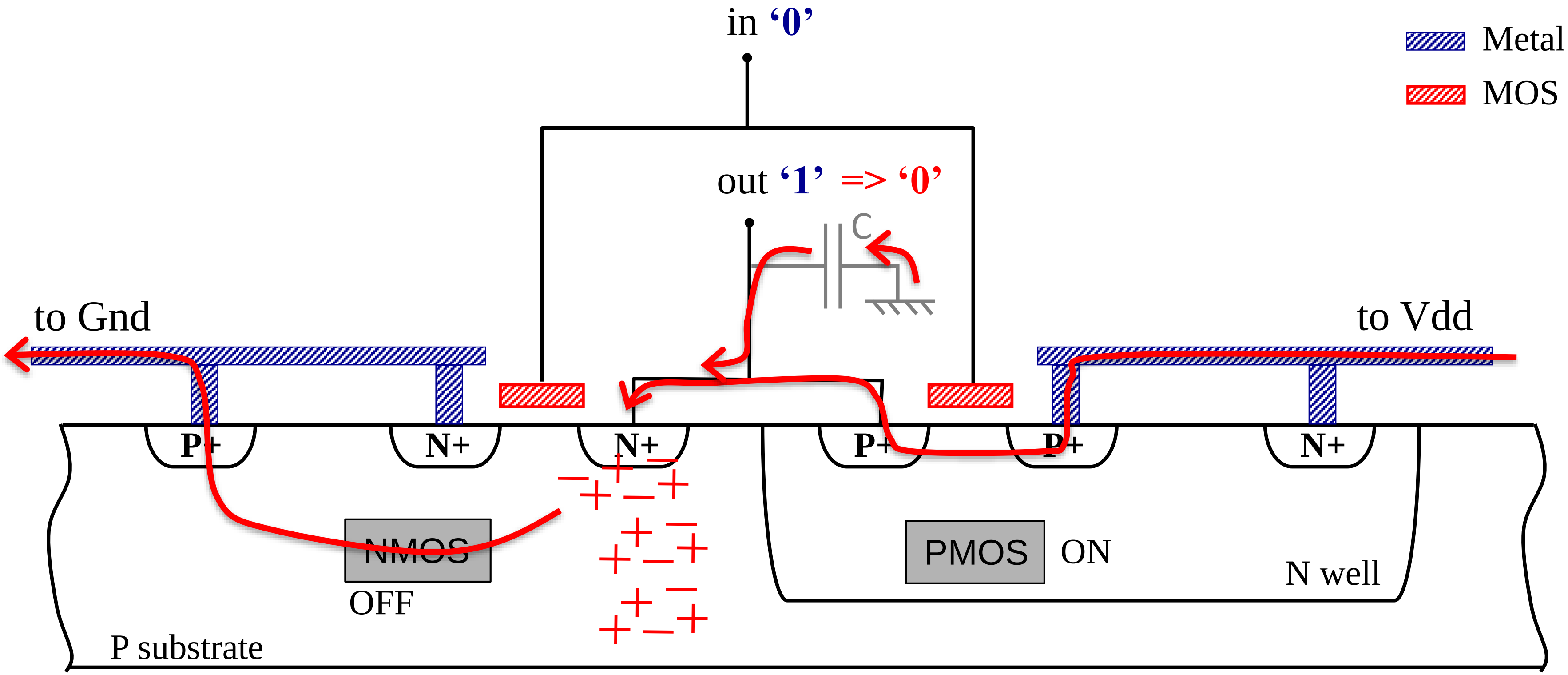
- Fault injection mechanism (the inverter case)

  from a transient current to a voltage transient (a.k.a. SET, single event transient)



- Fault injection mechanism (the inverter case)

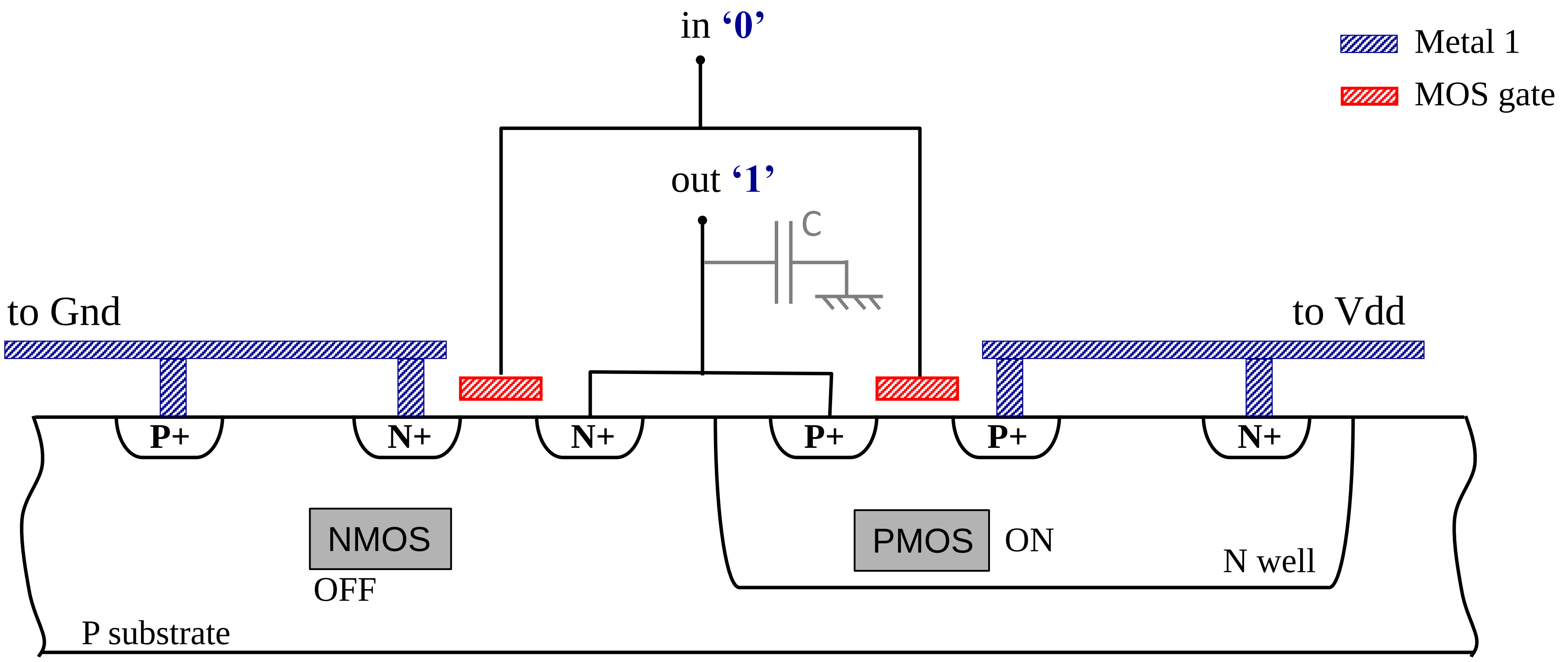
  from a transient current to a voltage transient (a.k.a. SET, single event transient)



II. Theory of laser fault injection

- Fault injection mechanism (the inverter case)

  from a transient current to a voltage transient (a.k.a. SET, single event transient)



Laser sensitive areas: OFF transistors' drains (reversed biased PN junctions)

II. Theory of laser fault injection

- Fault injection mechanism

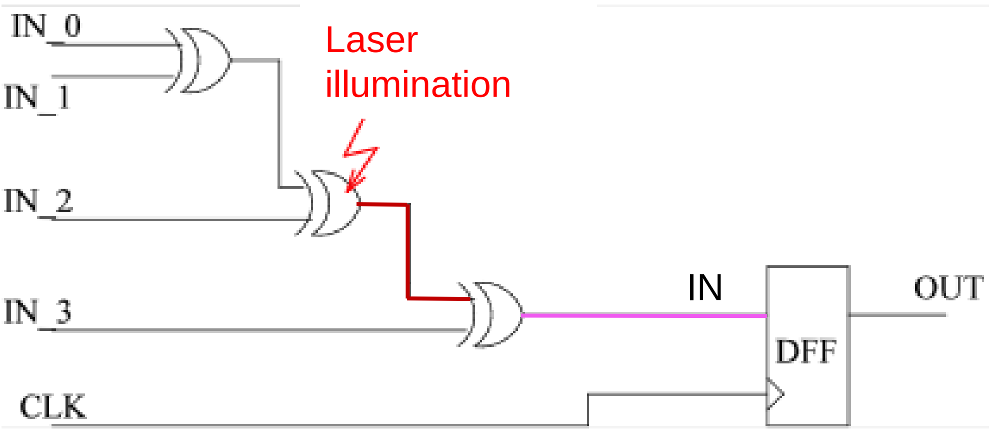
  from a voltage transient to an actual fault

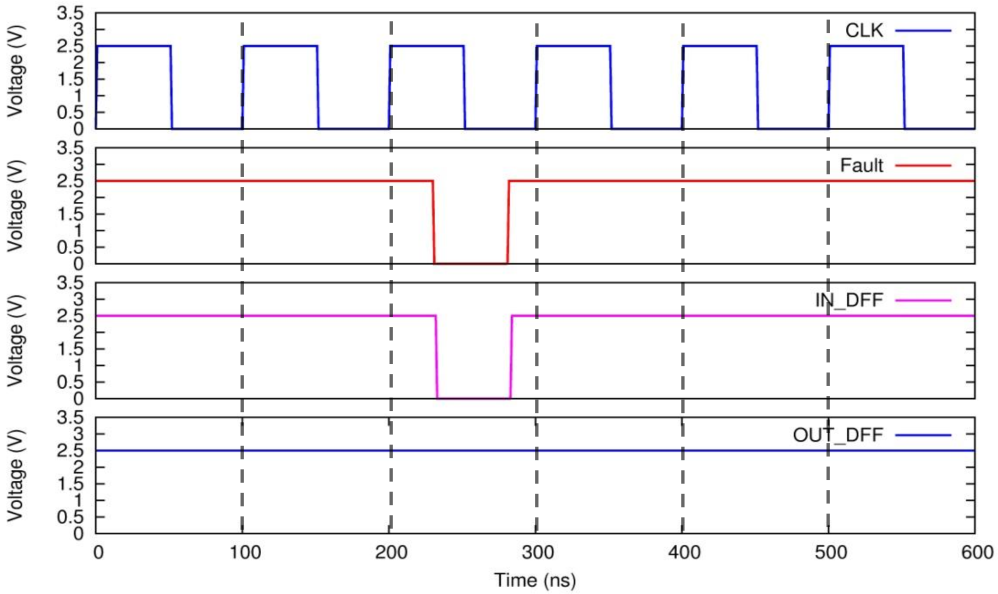
  Two mechanisms depending on the voltage transient location:

  1. logic,
  2. memory element (D flip-flop, SRAM)

- Fault injection mechanism – target: combinatorial logic

  from voltage transient to fault

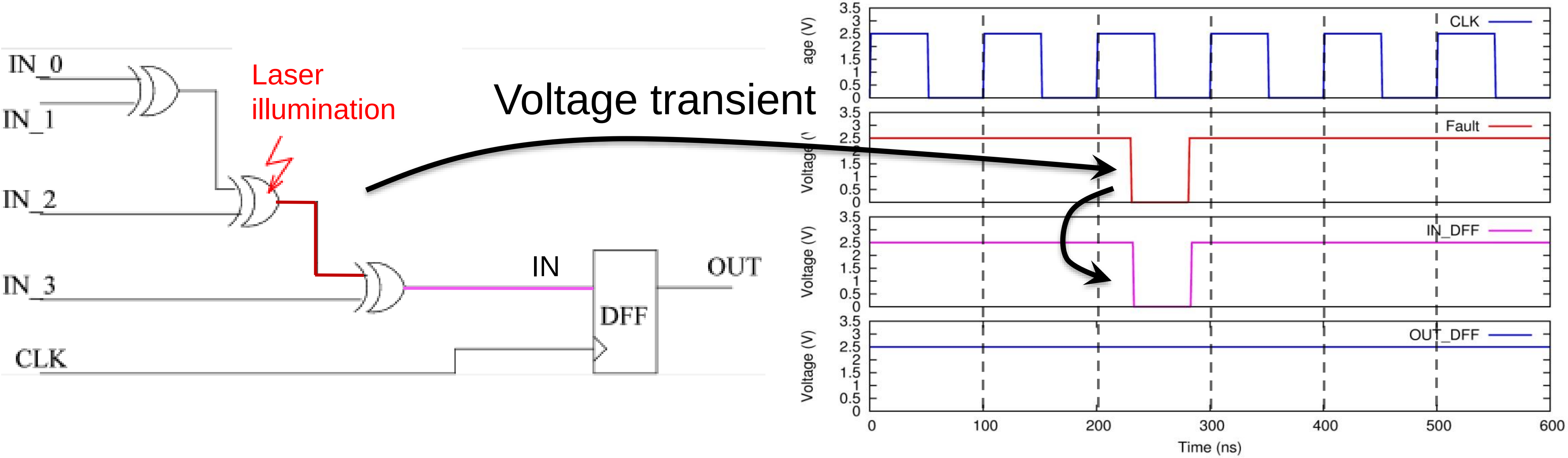




II. Theory of laser fault injection

- Fault injection mechanism – target: combinatorial logic

  from voltage transient to fault



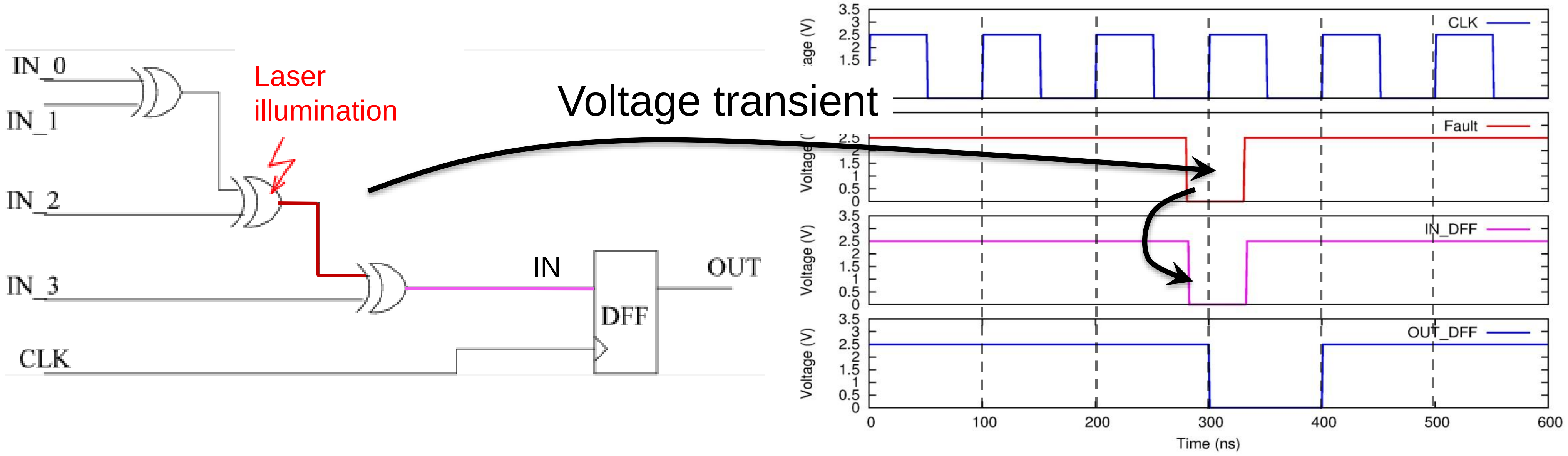
Laser illumination

Voltage transient

II. Theory of laser fault injection

- Fault injection mechanism – target: combinatorial logic

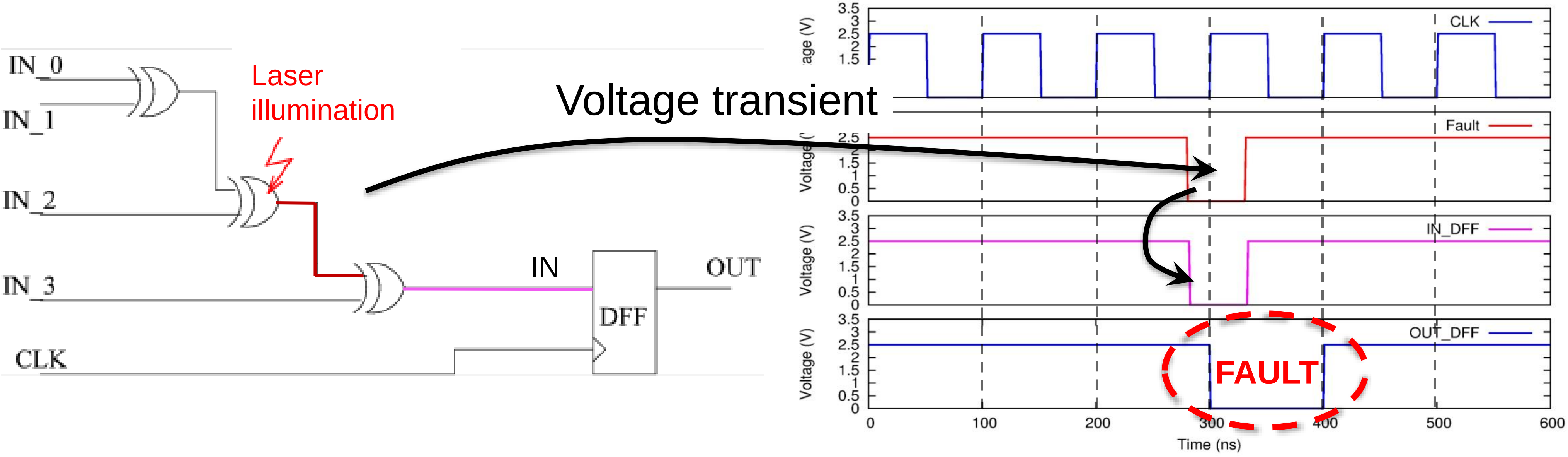
  from voltage transient to fault



II. Theory of laser fault injection

- Fault injection mechanism – target: combinatorial logic

  from voltage transient to fault



Laser illumination

Voltage transient

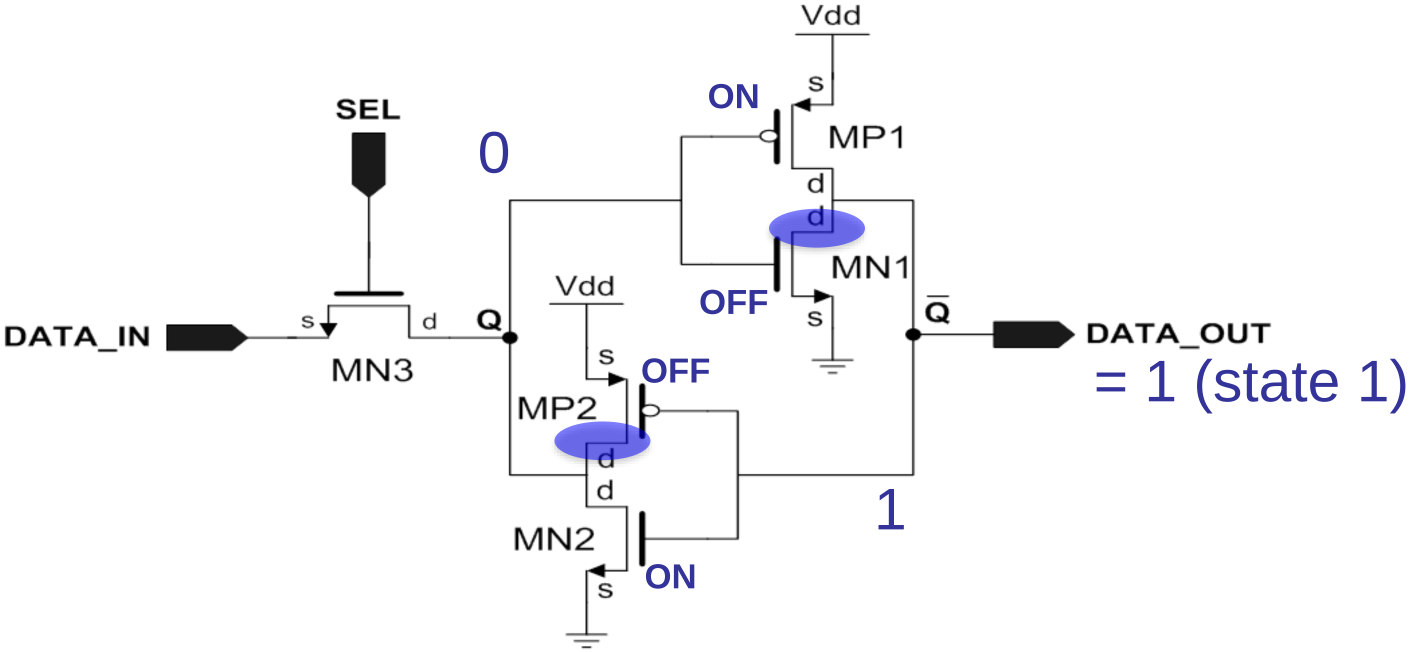
FAULT

The fault injection process depends both on:

- the injection time,
- the voltage transient duration.

- Fault injection mechanism – target: memory element (SRAM cell)

  from voltage transient to fault (SEU: single event upset)

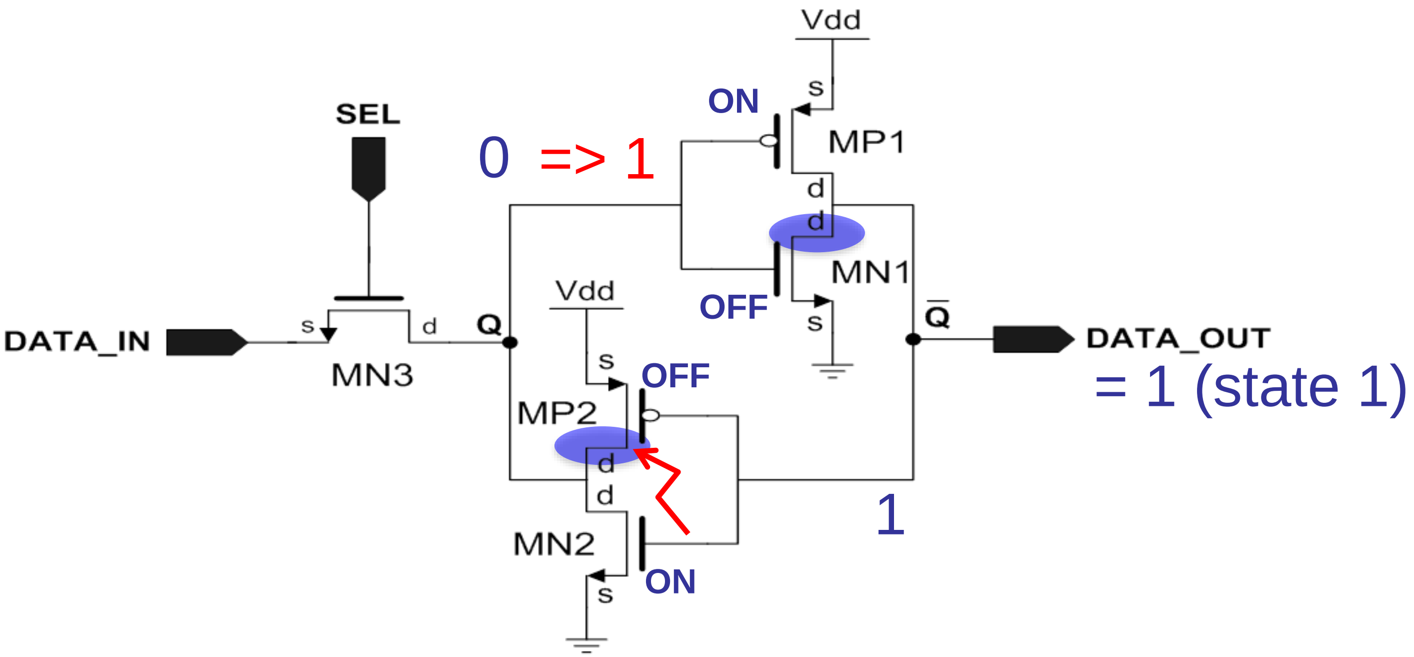


● laser sensitive area in state 1 (data dependent location)

II. Theory of laser fault injection

- Fault injection mechanism – target: memory element (SRAM cell)

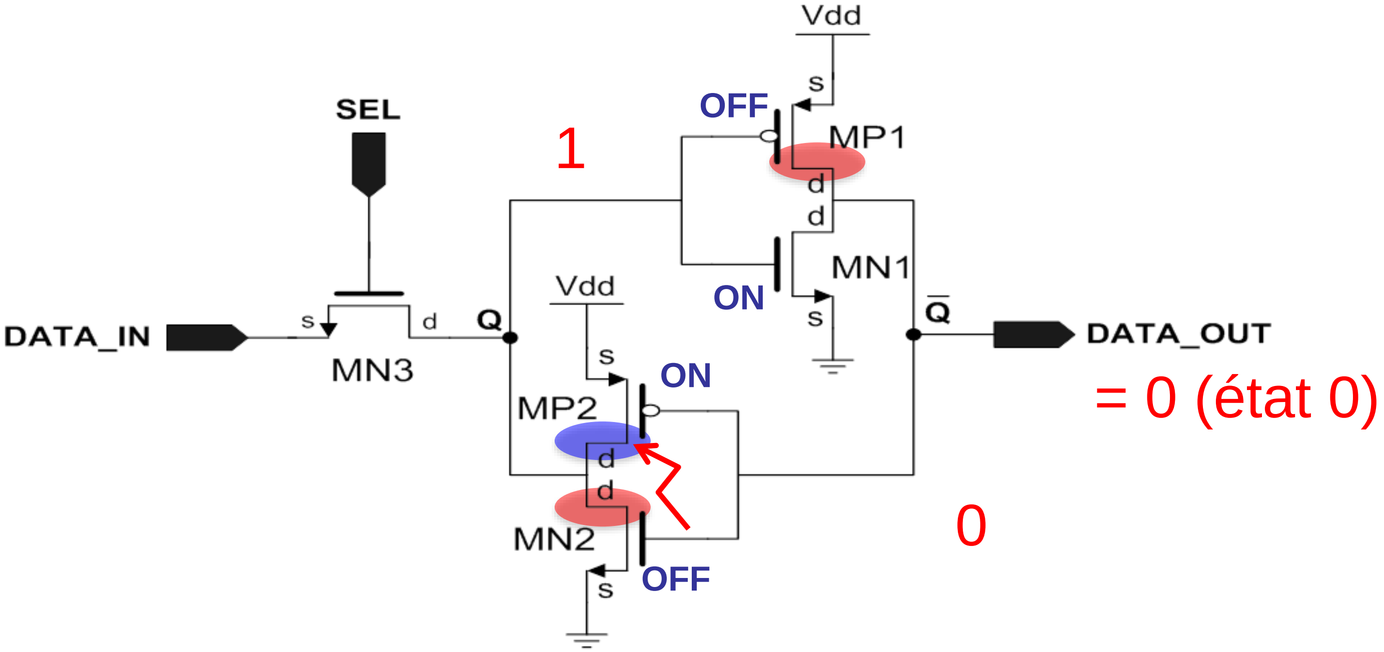
  from voltage transient to fault (SEU: single event upset)



● laser sensitive area in state 1 (data dependent location)

II. Theory of laser fault injection

- Fault injection mechanism – target: memory element (SRAM cell)
  from voltage transient to fault (SEU: single event upset)

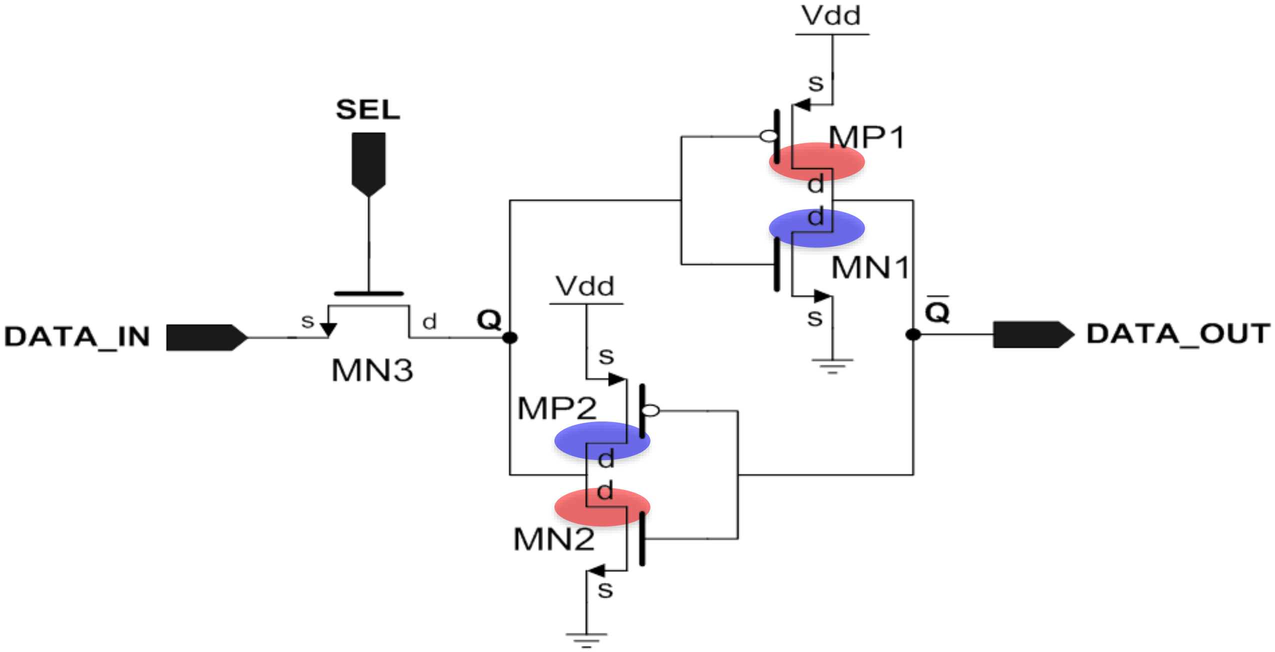


● laser sensitive area in state 1 (data dependent location)

● laser sensitive area in state 0 (data dependent location)

II. Theory of laser fault injection

- Fault injection mechanism – target: memory element (SRAM cell)
  from voltage transient to fault (SEU: single event upset)



🔵 laser sensitive area in state 1 (data dependent location)

🔴 laser sensitive area in state 0 (data dependent location)

Agenda

I. Introduction

Hardware attacks

II. Theory of laser fault injection

Physics and basics of laser fault injection

Fault models of laser injection

III. Practice of laser fault injection

Laser fault injection bench

Questions raised by technological advances

Experiment results (from CMOS 350 nm to 28 nm)

IV. Conclusion

❑ Fault model:

- requirements to be fulfilled to succeed in a given fault attack scheme

Often expressed as the number of faulted bits and the injection time, e.g.:

- Giraud DFA on AES (single bit, 9th round)
- Piret et al. DFA on AES (single byte, between last two MixColumns)

- remember that a fault attack consists in:

Disturbing the target’s nominal operating conditions in order to induce an abnormal behavior/calculation (ie injecting a fault)

while satisfying the fault model and without destroying the target.

❑ Fault model: mathematical expression at bit level

- bit-flip (usual fault model, data independent)

$$b \rightarrow not(b)$$

❑ Fault model: mathematical expression at bit level

- bit-set/reset fault model (data dependent)

$$\left.\begin{array}{l} if\ \ b = 0 \rightarrow \boxed{b = 1} \\ if\ \ b = 1 \rightarrow b = 1 \end{array}\right\} \text{bit-set}$$

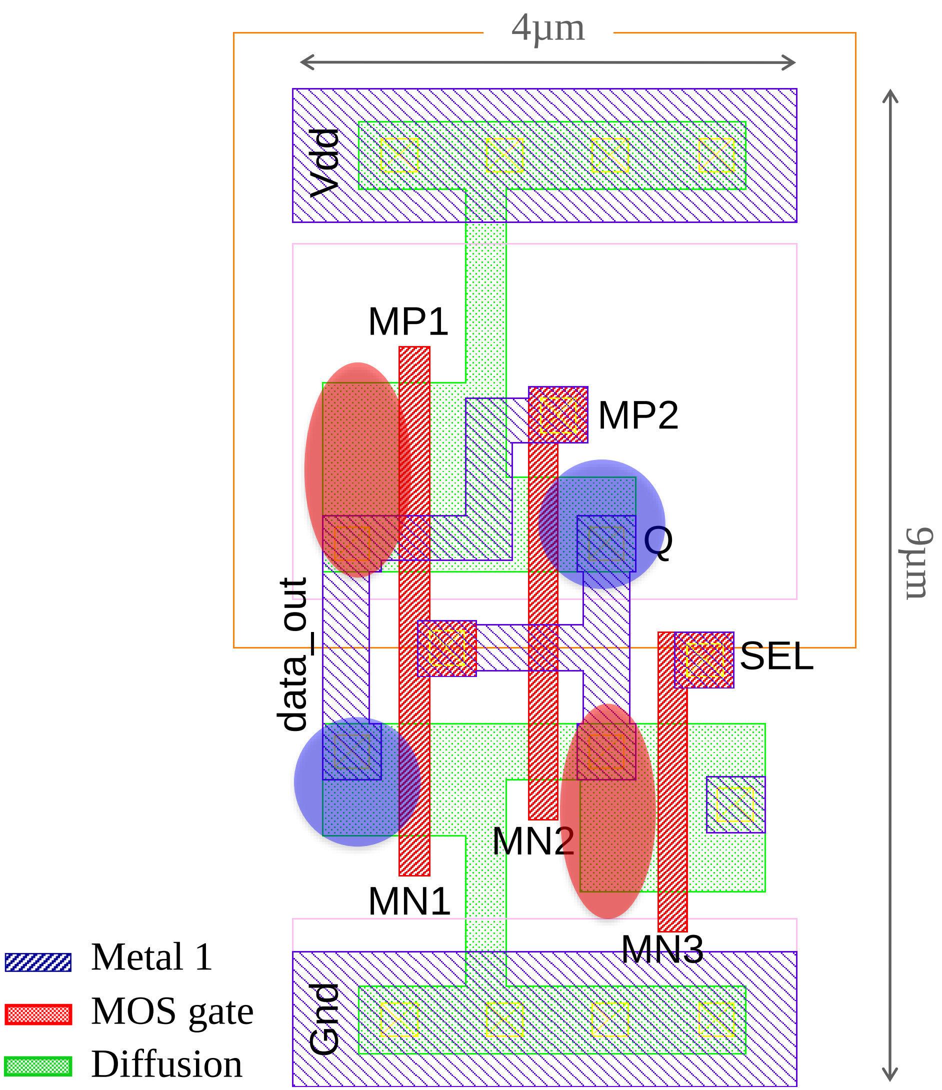
$$\left.\begin{array}{l} if\ \ b = 0 \rightarrow b = 0 \\ if\ \ b = 1 \rightarrow \boxed{b = 0} \end{array}\right\} \text{bit-reset}$$

Provide **additional information** on the original bit value

⇨ Safe error attack (e.g. retrieveing memory bits)

II. Theory of laser fault injection

- bit-set/reset fault model of memory elements: 5T SRAM cell

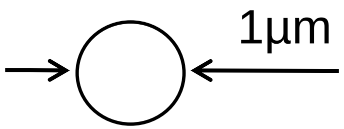


Laser sensitive areas:

● state 1

● state 0

Laser spot size/effect area:

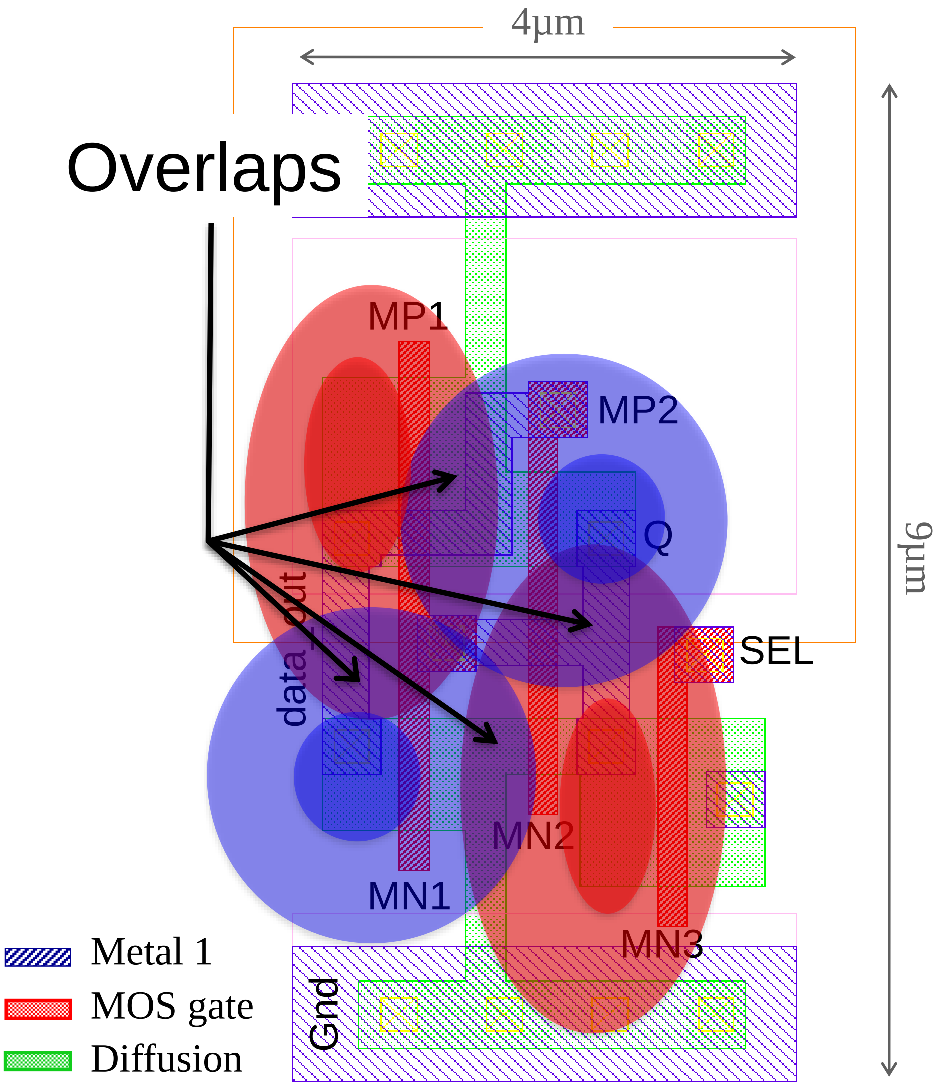


One laser sensitive area exposed

⇨ bit-set/reset fault model

II. Theory of laser fault injection

- bit-set/reset fault model of memory elements: 5T SRAM cell

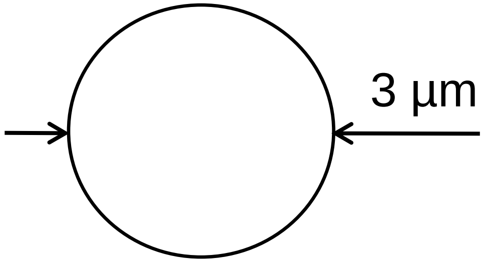


Laser sensitive areas:

🔵 state 1

🔴 state 0

Laser spot size/effect area:



Overlaps of laser sensitive areas

⇨ bit-flip fault model

II. Theory of laser fault injection

- bit-set/reset fault model of memory elements: 5T SRAM cell

Q? fault model of memory elements:

- bit-flip, data independent
- bit-set/reset, data dependent (safe error attacks)

- other fault model issues

Q? feasibility of single bit/byte fault model

Q? with respect to technology shrinkage

Agenda

I. Introduction

Hardware attacks

II. Theory of laser fault injection

Physics and basics of laser fault injection

Fault models of laser injection

III. Practice of laser fault injection

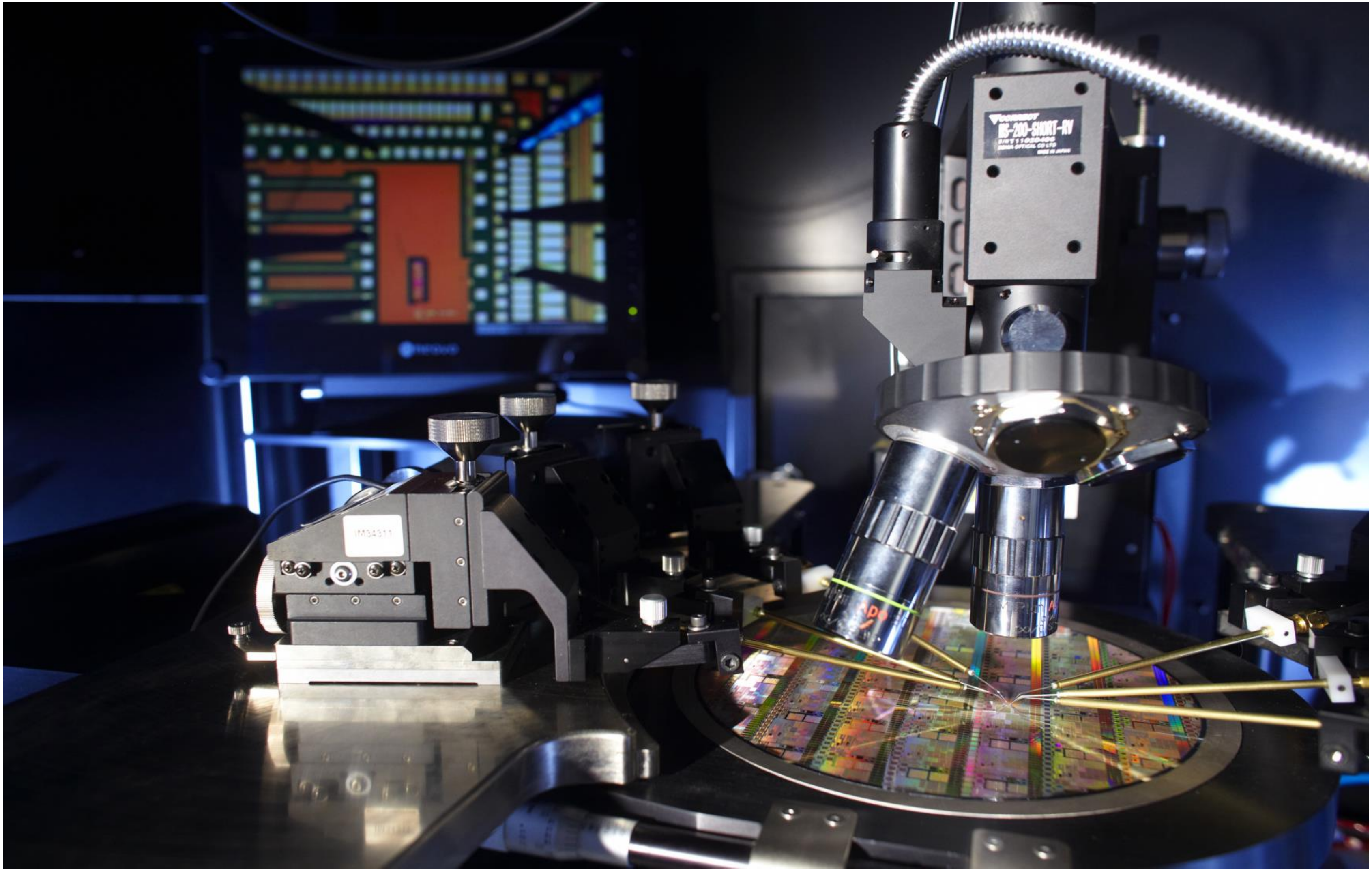
Laser fault injection bench

Questions raised by technological advances

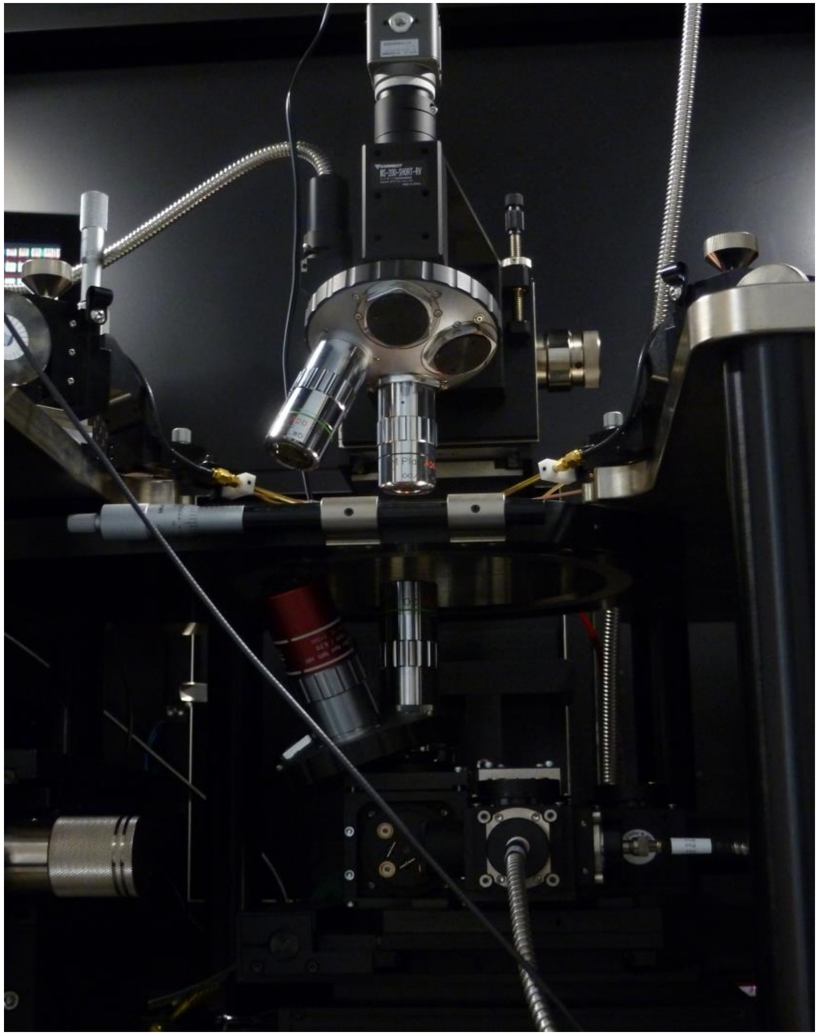
Experiment results (from CMOS 350 nm to 28 nm)

IV. Conclusion

❑ Laser fault injection bench



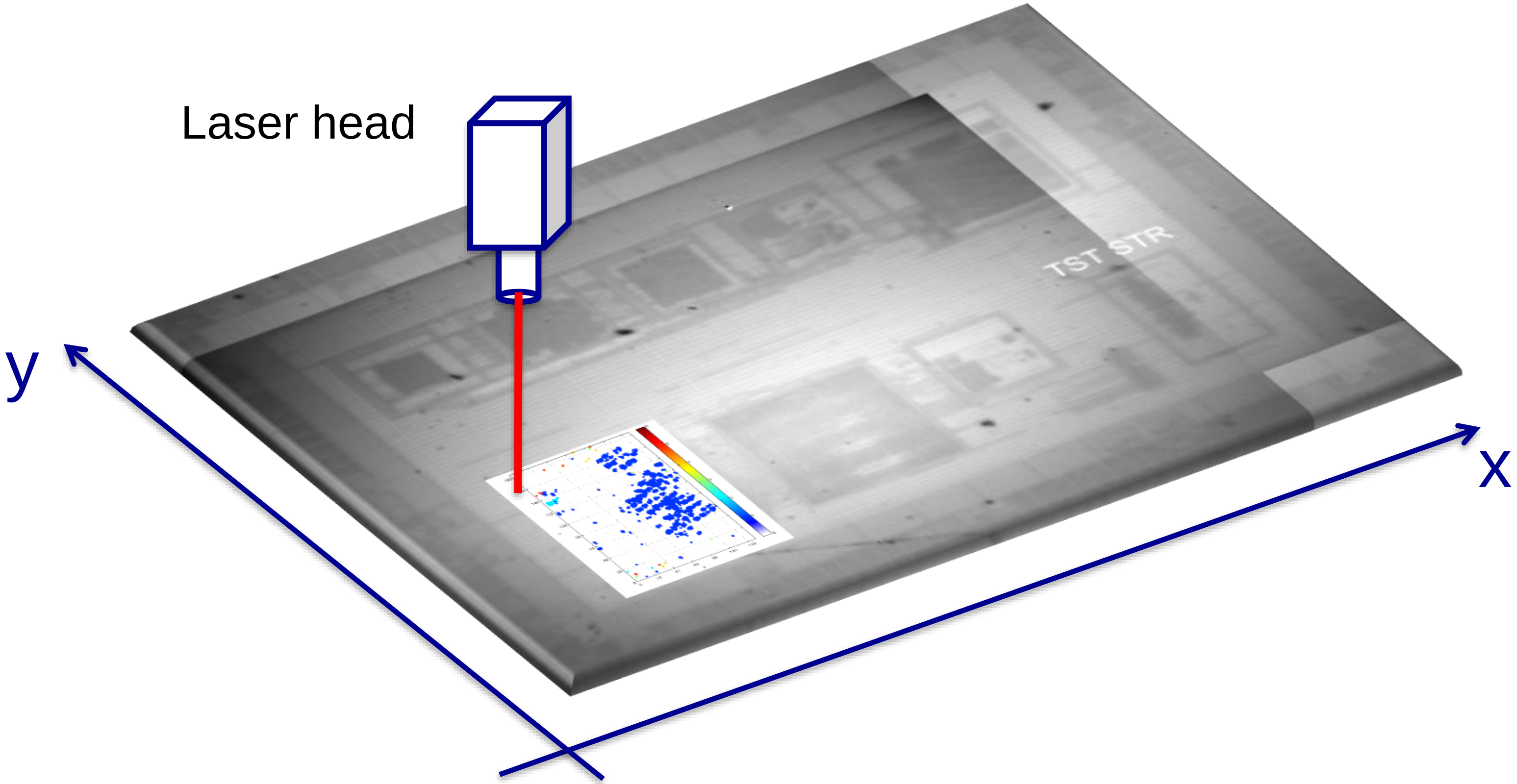
❑ Laser fault injection bench



- Frontside/backside injection
- Wavelength: 1064nm & 1030nm (IR)
- Spot size: 1 – 20µm
- Pulse width: 30ps or 5ns – 1s
- Energy max: 100nJ or 25W
- XYZ stage: 0.1µm resolution
- Jitter: < 1ns

- IR camera
- XYZ stages
- Laser output (photodiode)

❑ Laser fault injection bench: laser sensitivity maps



Agenda

I. Introduction

Hardware attacks

II. Theory of laser fault injection

Physics and basics of laser fault injection

Fault models of laser injection

III. Practice of laser fault injection

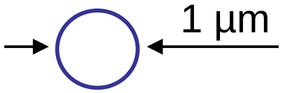
Laser fault injection bench

Questions raised by technological advances

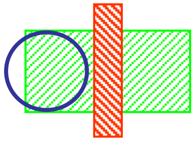
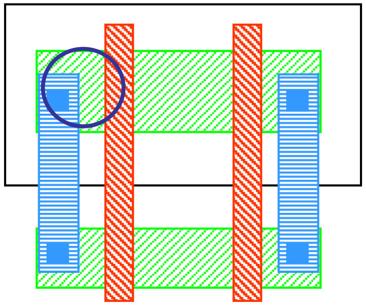
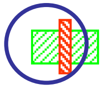
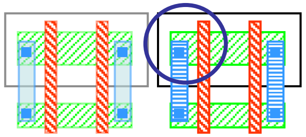
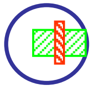
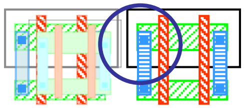
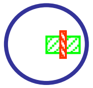
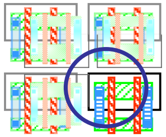
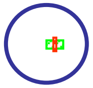
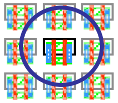
Experiment results (from CMOS 350 nm to 28 nm)

IV. Conclusion

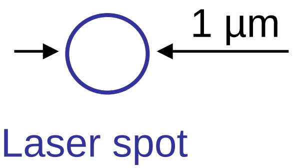
❑ Single-bit/byte fault model validity?

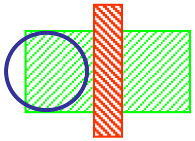
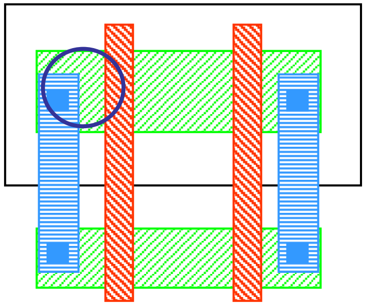
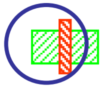
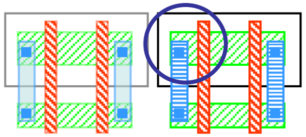
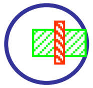
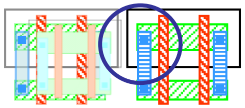
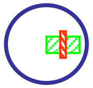
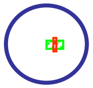
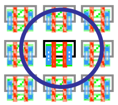


Laser spot

Technology	MOS transistor	SRAM
0.35 µm		
130 nm		
90 nm		
65 nm		
28 nm		

❑ Single-bit/byte fault model validity?



Technology	MOS transistor	SRAM
0.35 µm		
130 nm		
90 nm		
65 nm		
28 nm		

Simultaneous flip of several SRAMs?

Agenda

I. Introduction

II. Theory of laser fault injection

III. Practice of laser fault injection

Laser fault injection bench

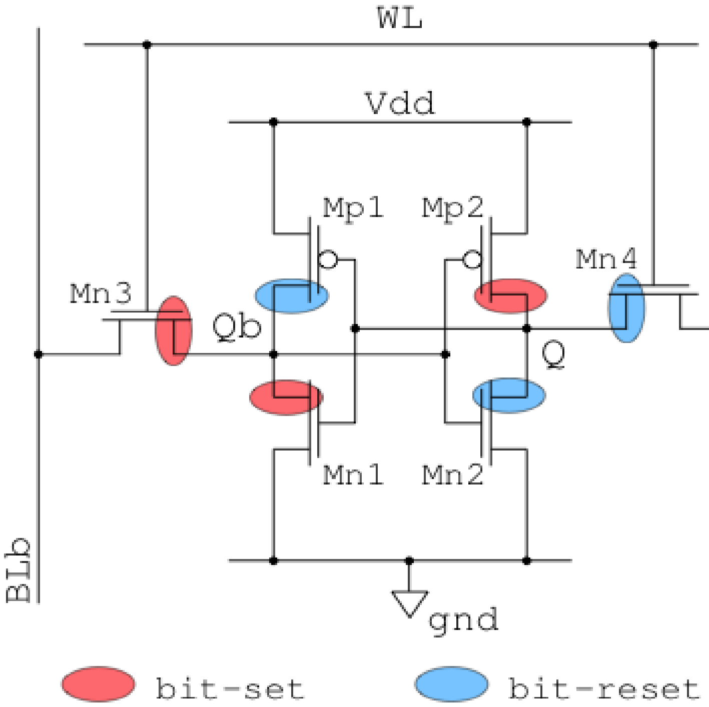
Questions raised by technological advances

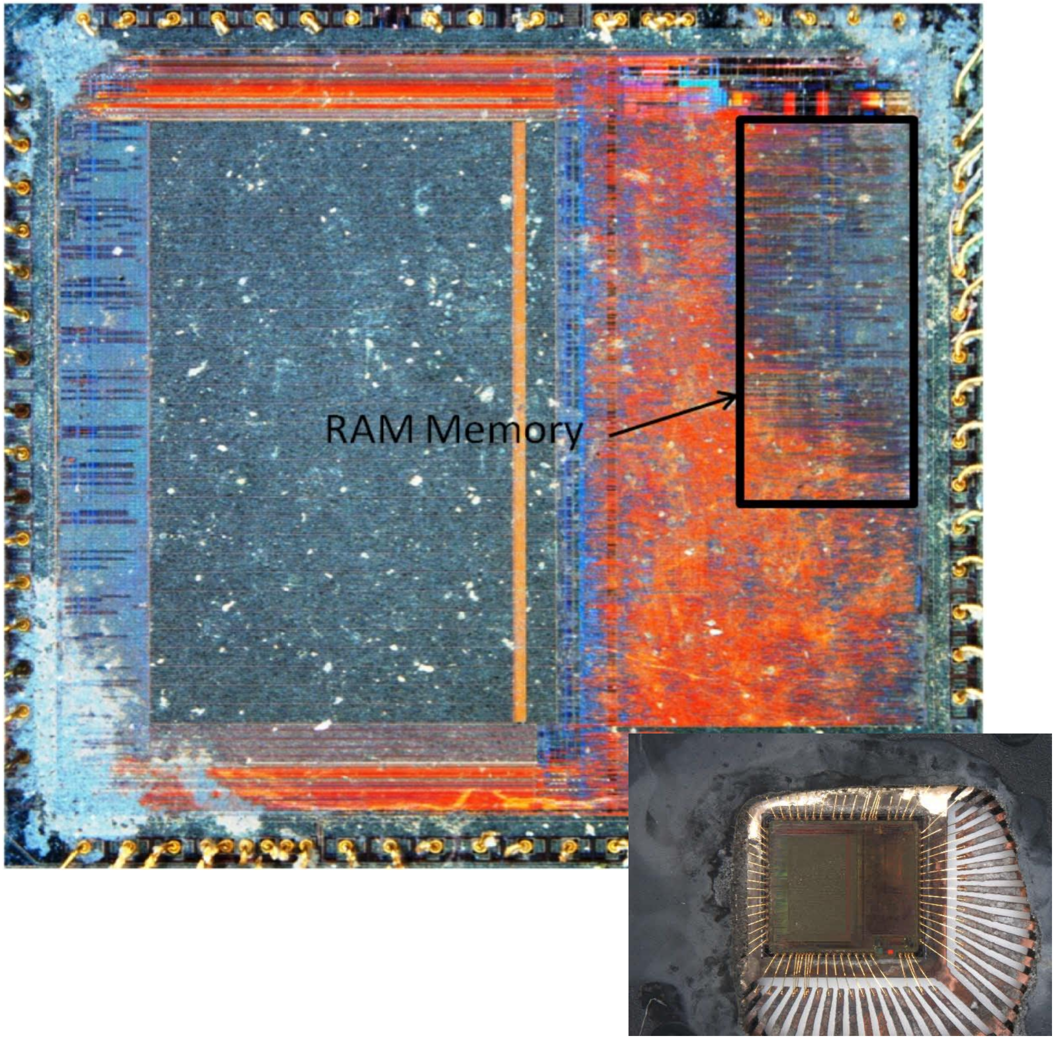
Experiment results (from CMOS 350 nm to 28 nm)

- memory elements
- microcontroller
- ASIC

IV. Conclusion

- RAM memory of an 8-bit µCTRL, CMOS 350 nm

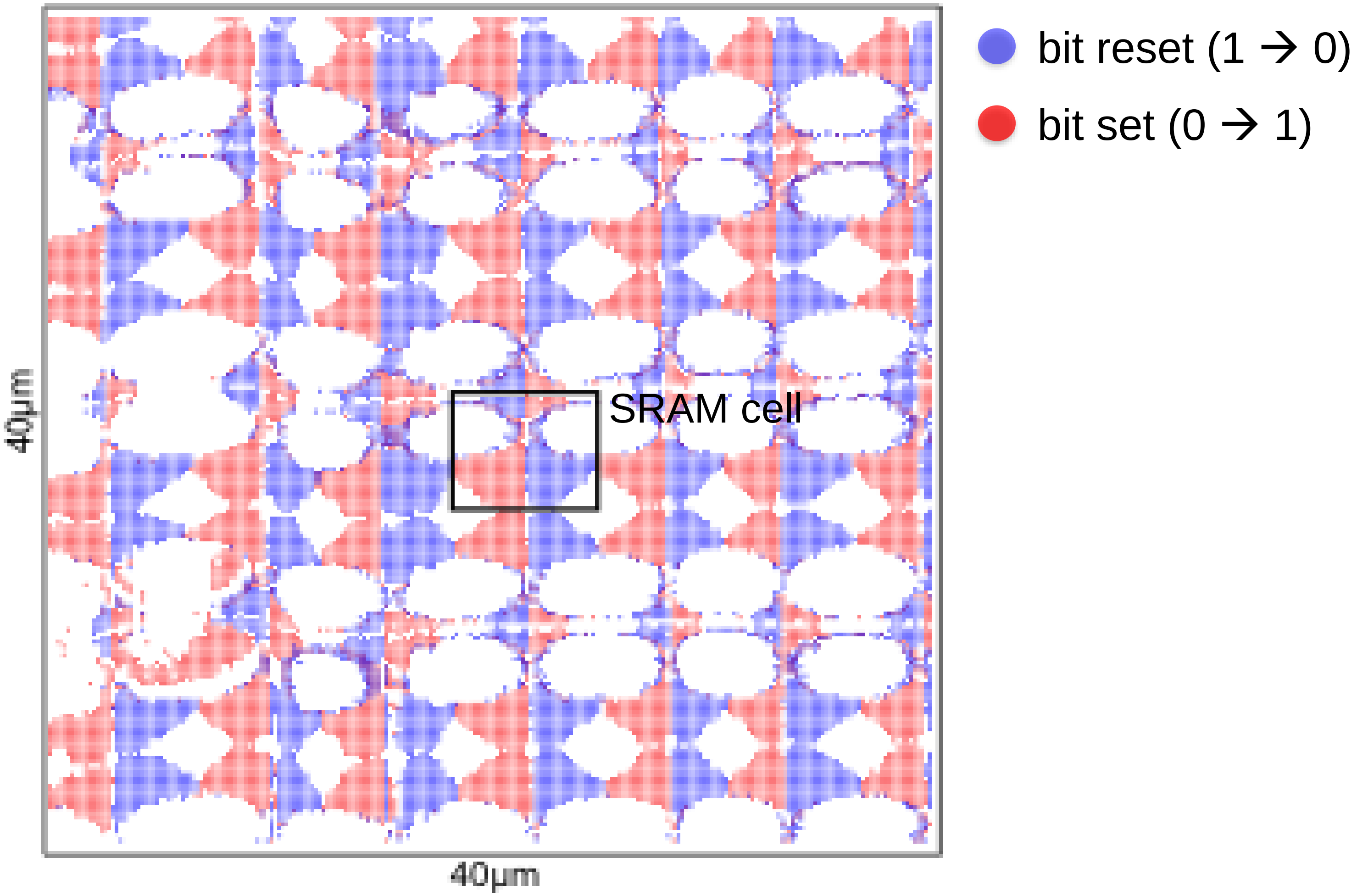




❑ RAM memory of an 8-bit µCTRL, CMOS 350 nm

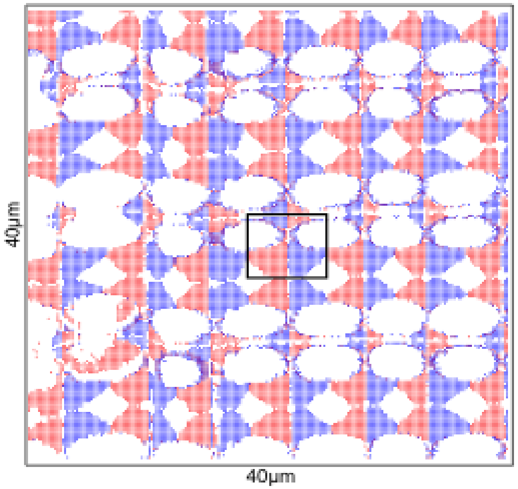
- spot 1 µm / **30 ps** / 2.4 nJ / Δxy = 0.2 µm / backside

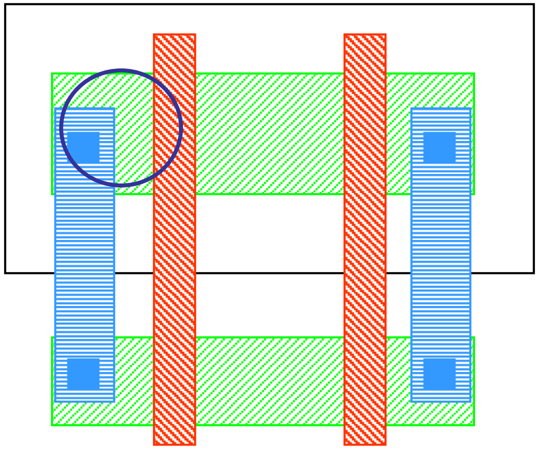
  Laser-sensitivity map

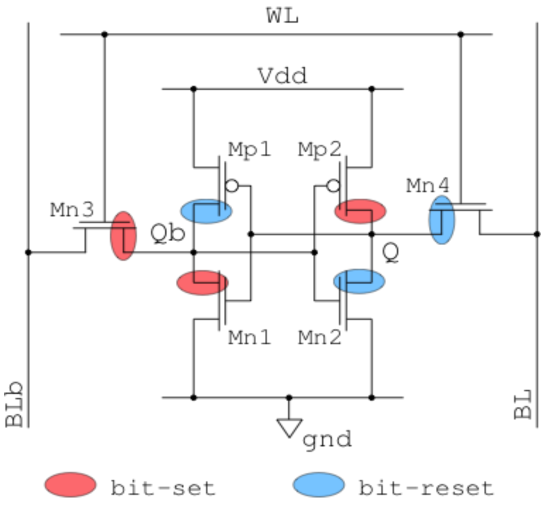


❑ RAM memory of an 8-bit µCTRL, CMOS 350 nm

- spot 1 µm / **30 ps** / 2.4 nJ / Δxy = 0.2 µm / backside







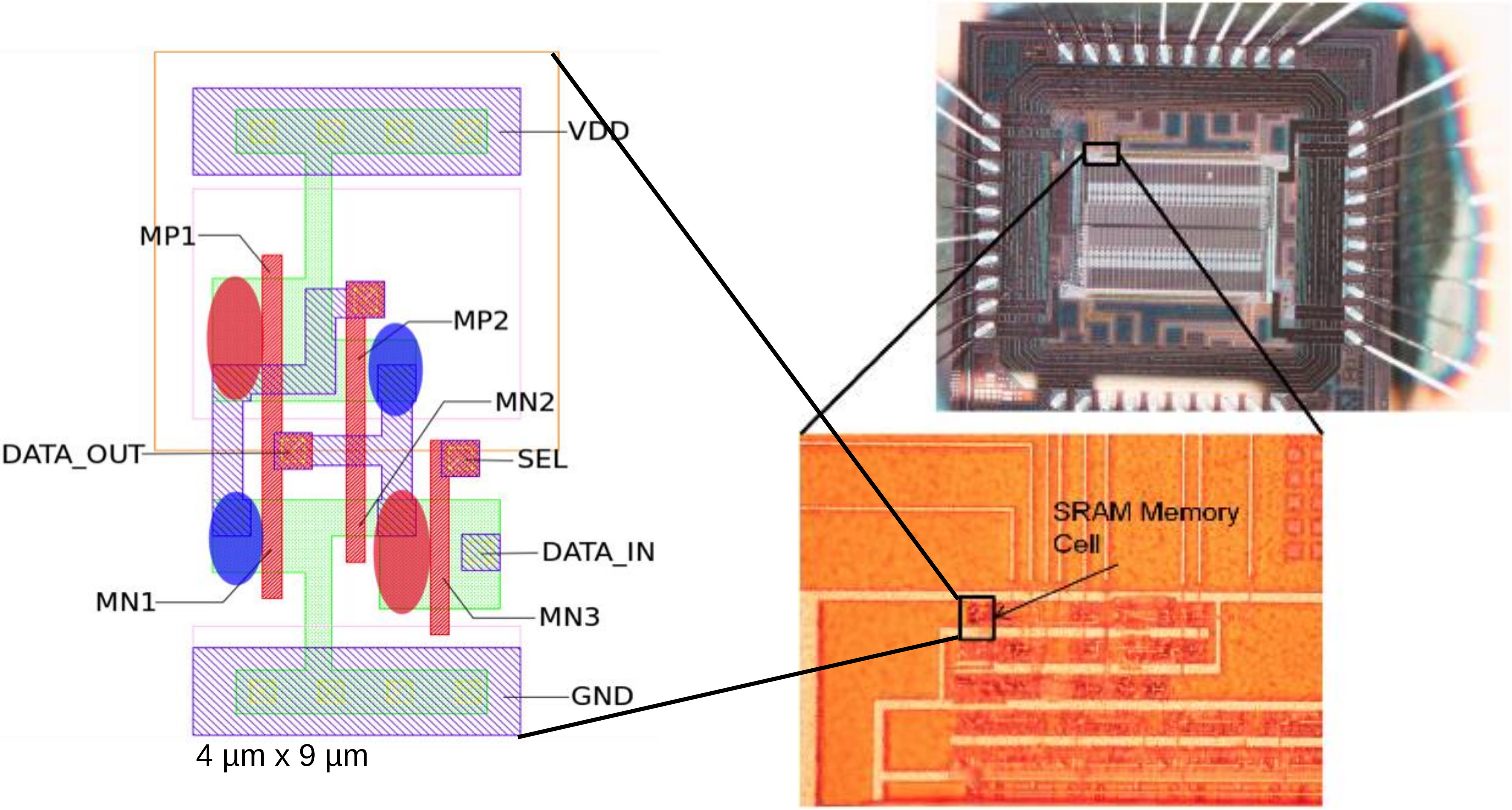
⇨ Single-bit fault model achieved

Consistent with the theory (4 sensitive areas)

C. Roscian, A. Sarafianos, J.-M. Dutertre, and A. Tria. Fault model analysis of laser-induced faults in SRAM memory cells. In 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography, 2013.

❑ Custom 5T SRAM cell, CMOS 250 nm

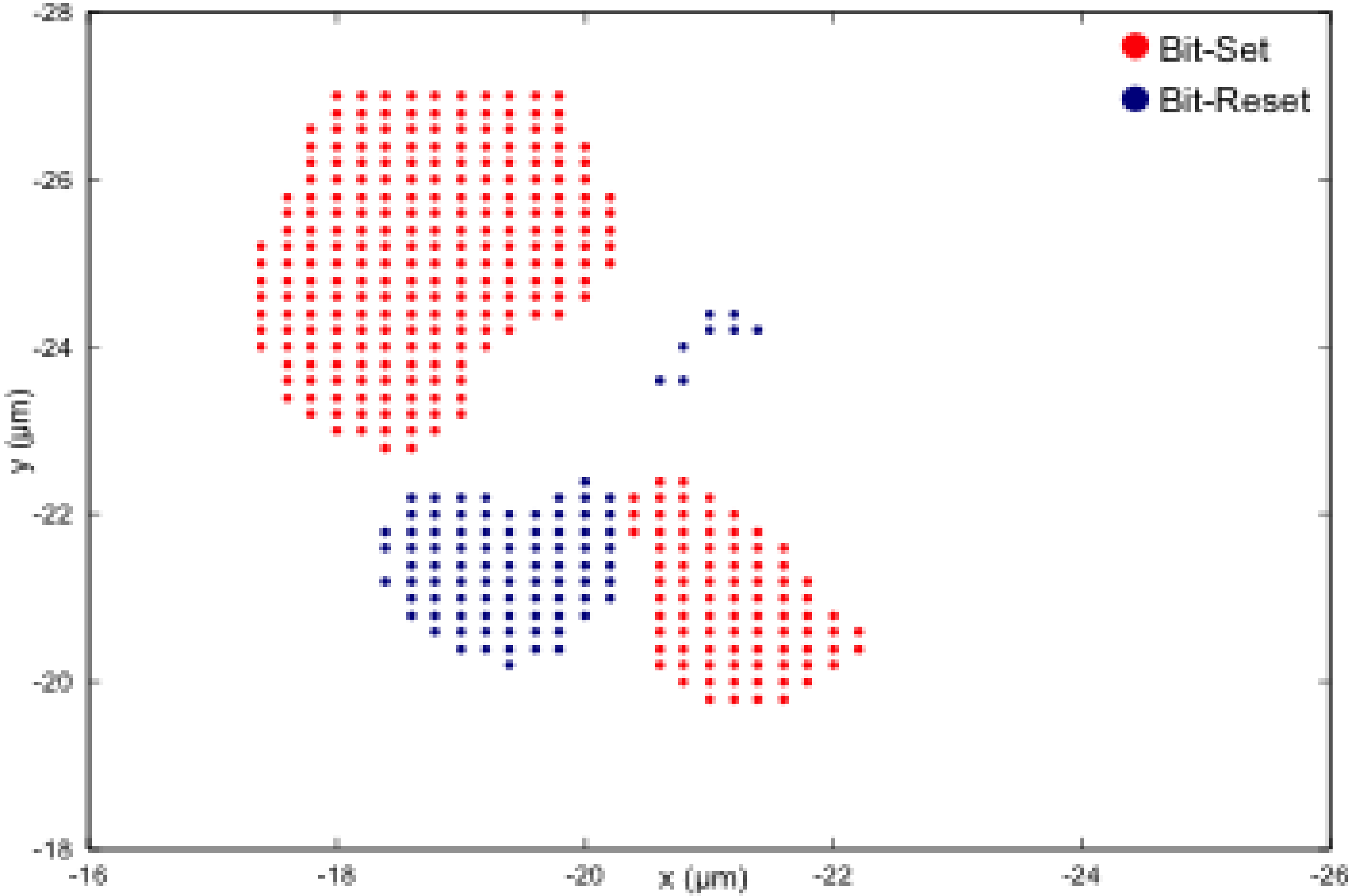
- spot 1 µm / **30 ps** / 3.2 nJ / Δxy = 0.2 µm / frontside



4 µm x 9 µm

❑ Custom 5T SRAM cell, CMOS 250 nm

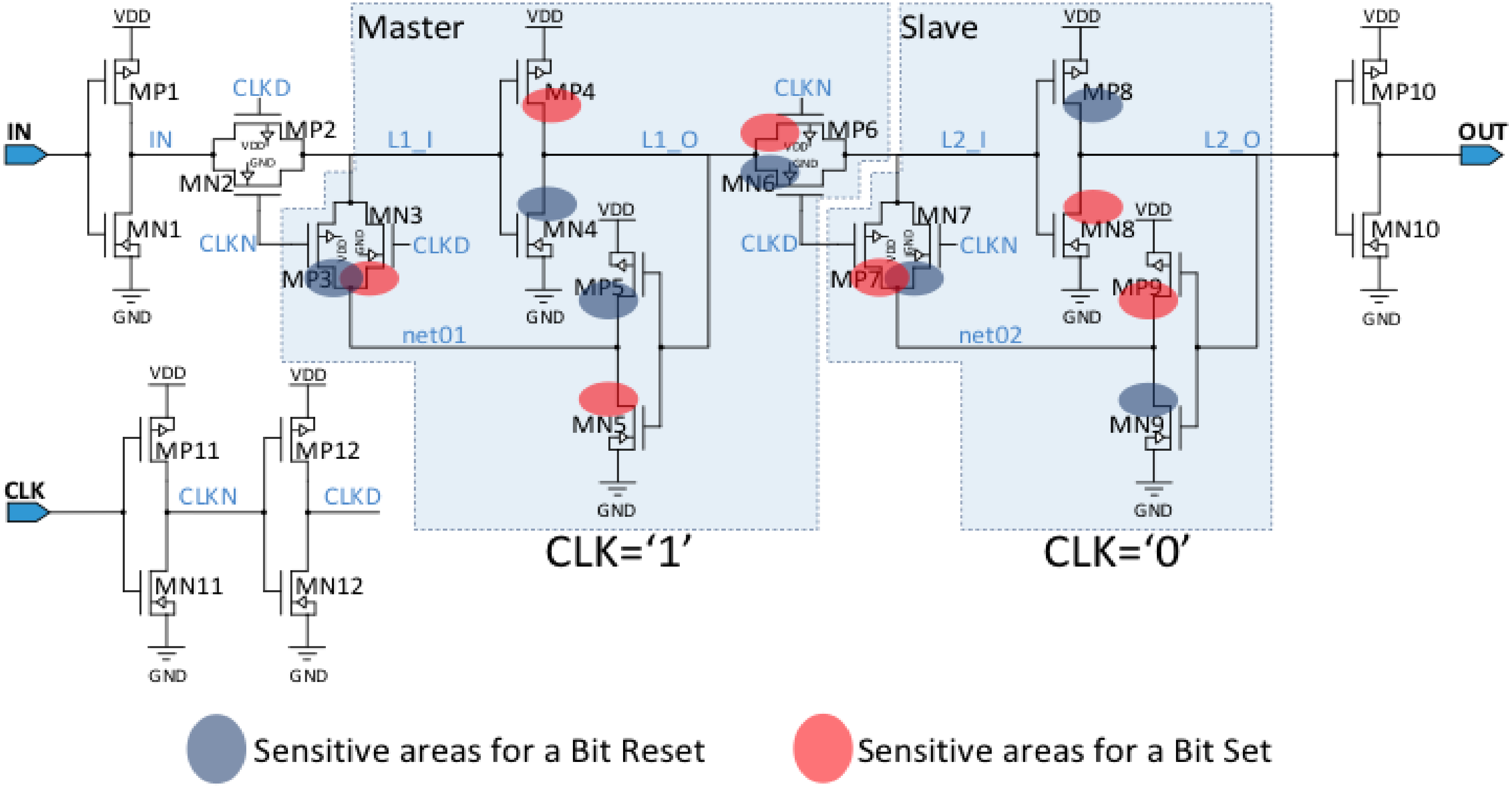
- spot 1 µm / **30 ps** / 3.2 nJ / Δxy = 0.2 µm / frontside



M. Lacruche, et al., Laser fault injection into SRAM cells: Picosecond versus nanosecond pulses. In On-Line Testing Symposium (IOLTS), 2015 IEEE 21st International, pages 13–18, July 2015.

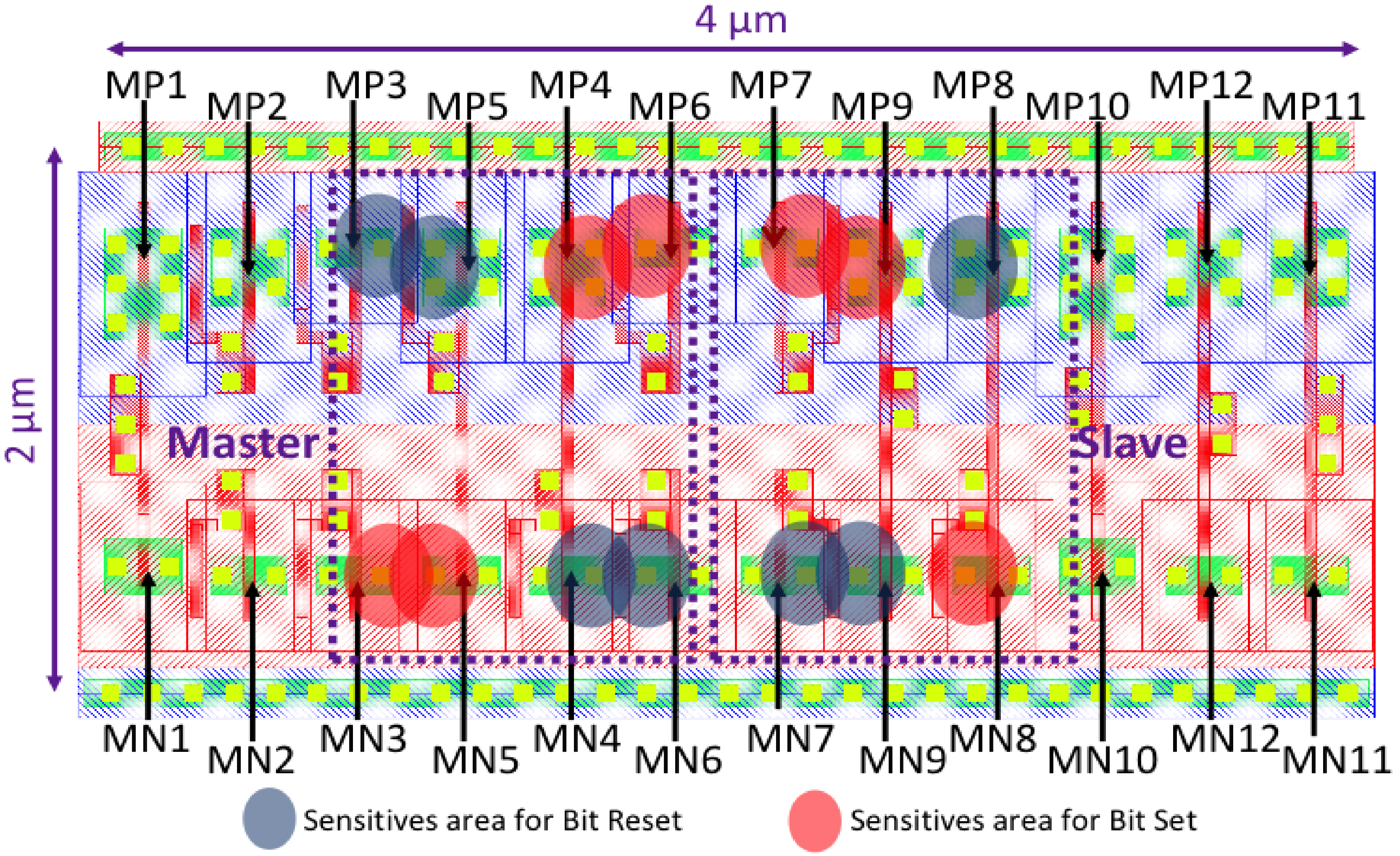
❑ Custom D flip-flop, CMOS 40 nm

- schematic



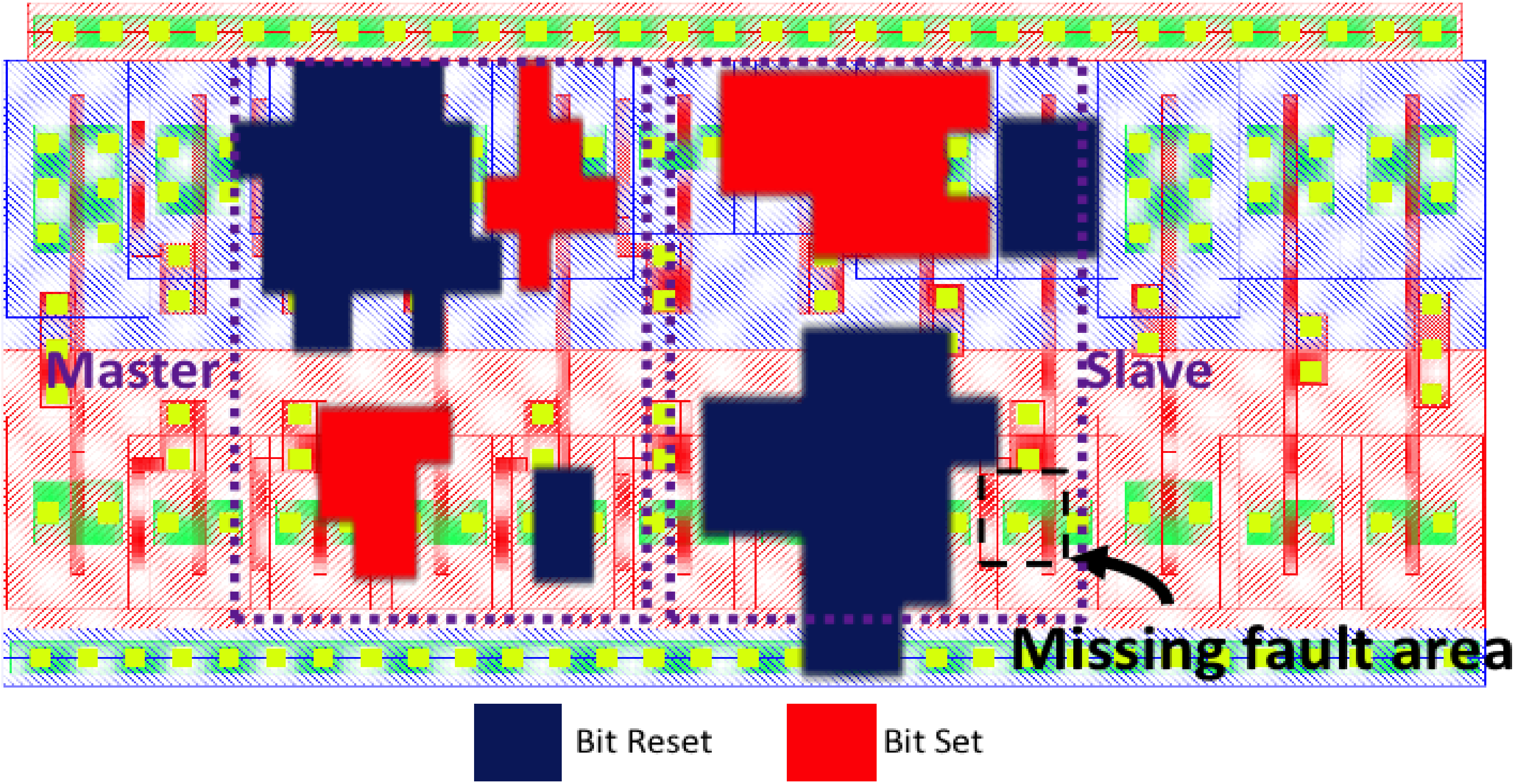
❑ Custom D flip-flop, CMOS 40 nm

- layout



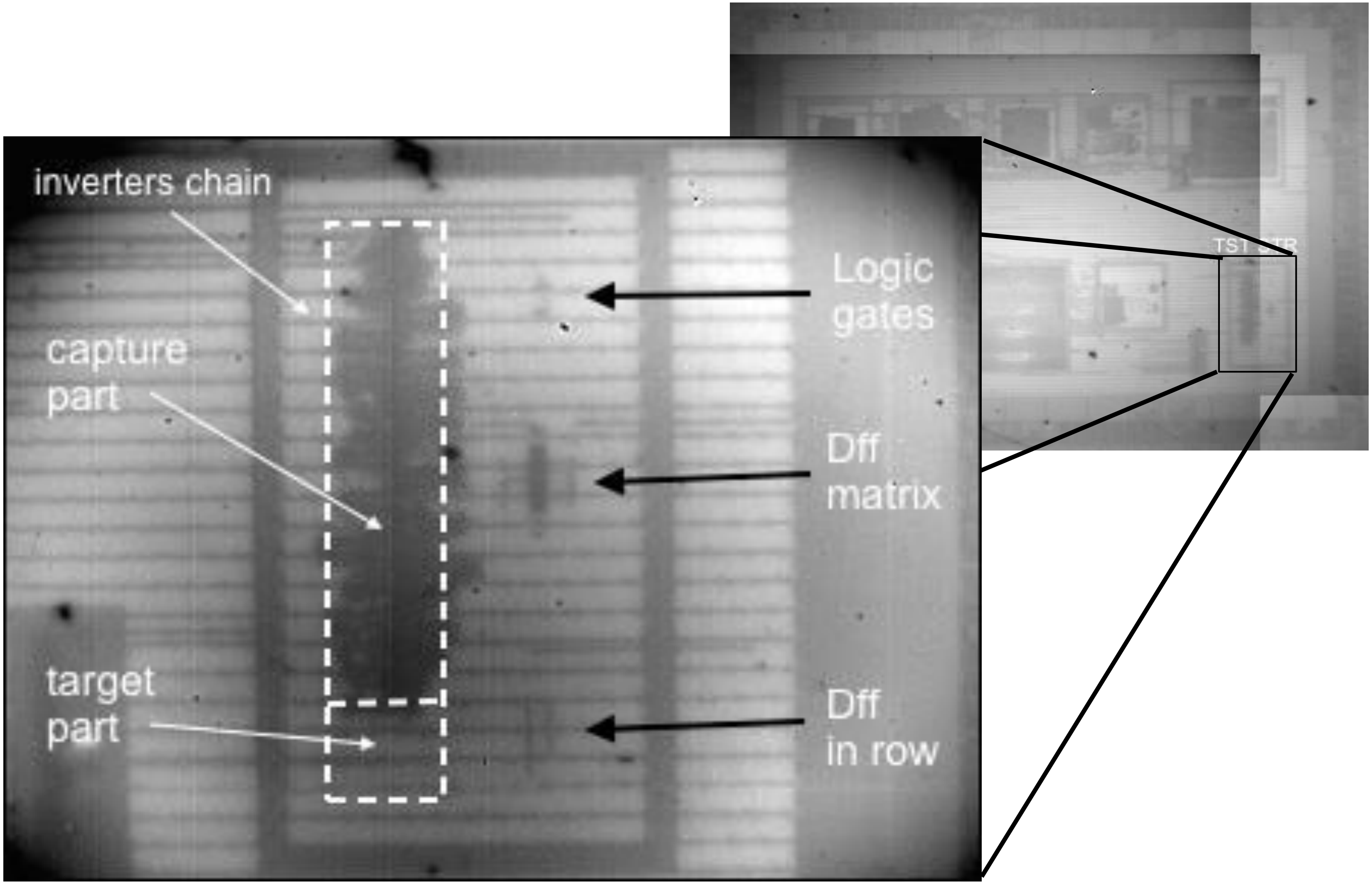
❑ Custom D flip-flop, CMOS 40 nm

- spot 1 µm / **30 ps** / 0.7 nJ / Δxy = 0,2 µm / backside



C. Champeix, et al., SEU sensitivity and modeling using pico-second pulsed laser stimulation of a D flip-flop in 40 nm CMOS technology. In Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS), 2015 IEEE International Symposium.

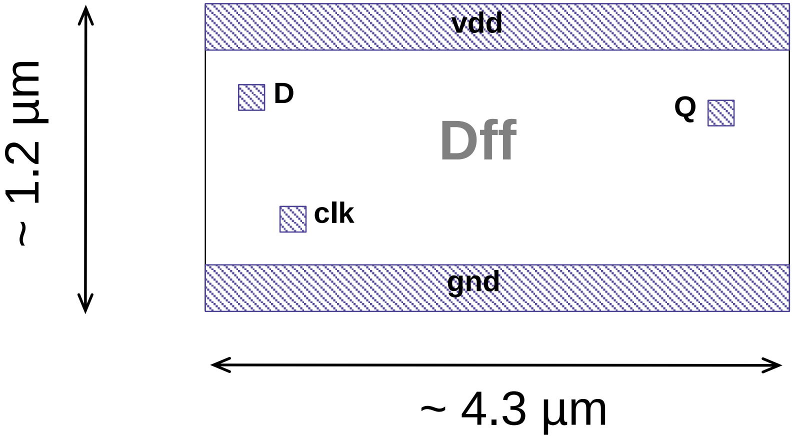
- Custom D flip-flop registers, CMOS 28 nm

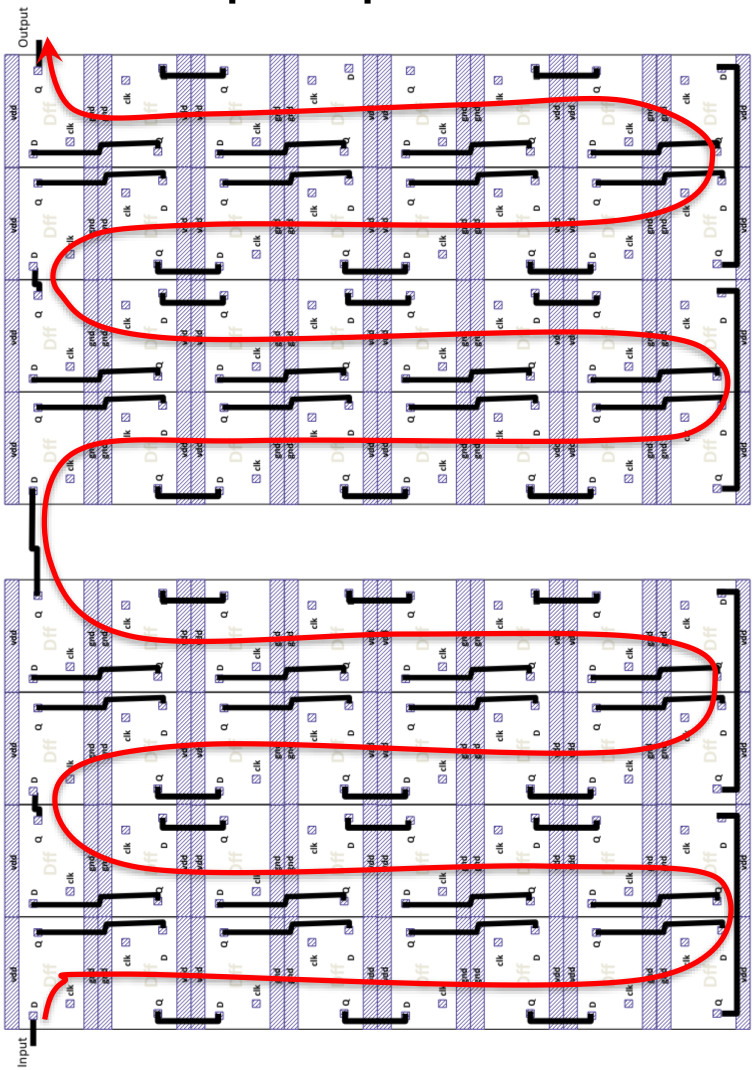


J.-M. Dutertre, et al., Assessment of the laser-induced fault model towards continuous cmos technology shrinkage. TRUDEVICE Workshop, Dresden Germany, March 2016.

❑ Custom D flip-flop registers, CMOS 28 nm

- Matrix shaped shift register with 64 D flip-flops

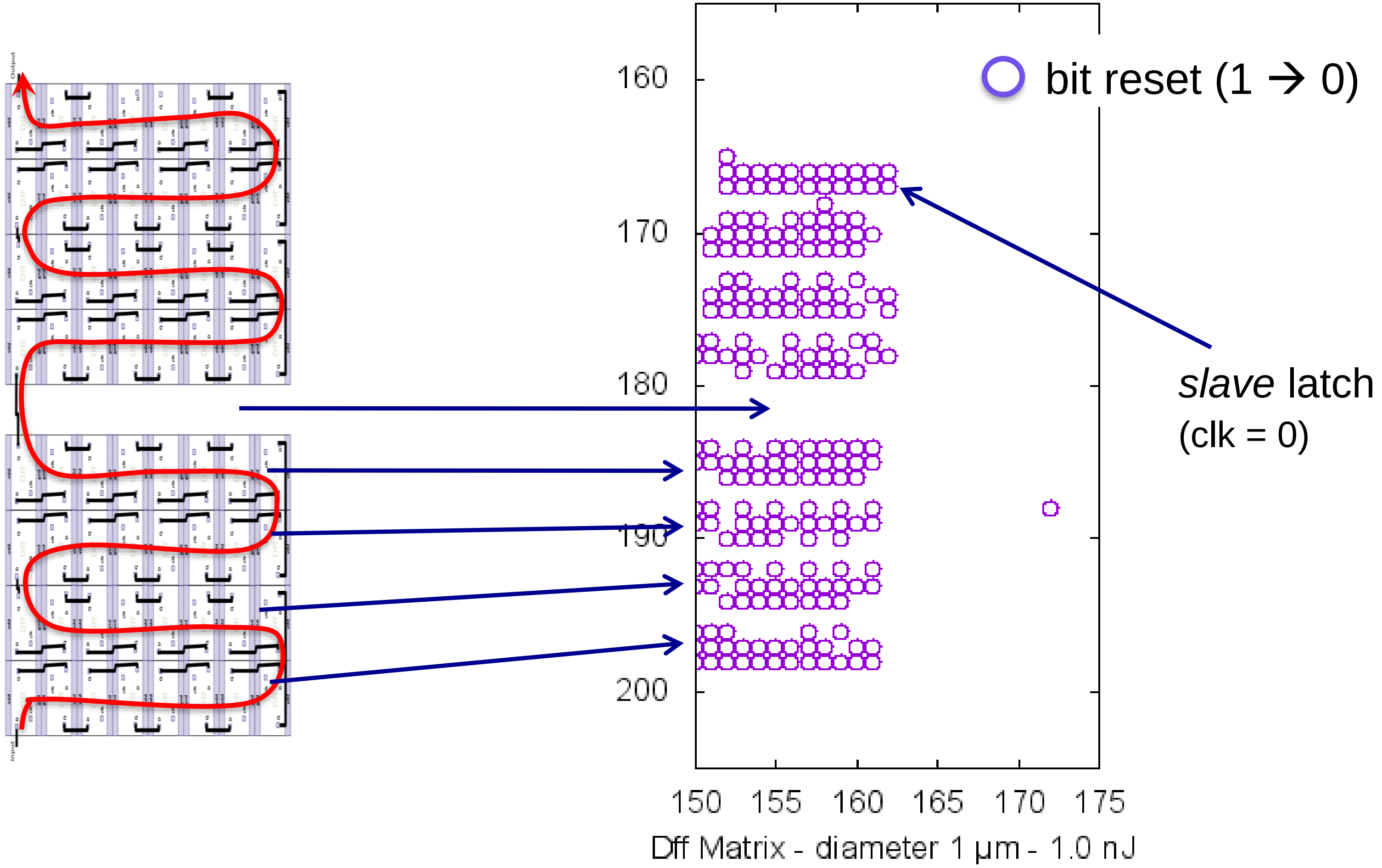




- DFF: ~ 40 transistors,

- *large* output buffer

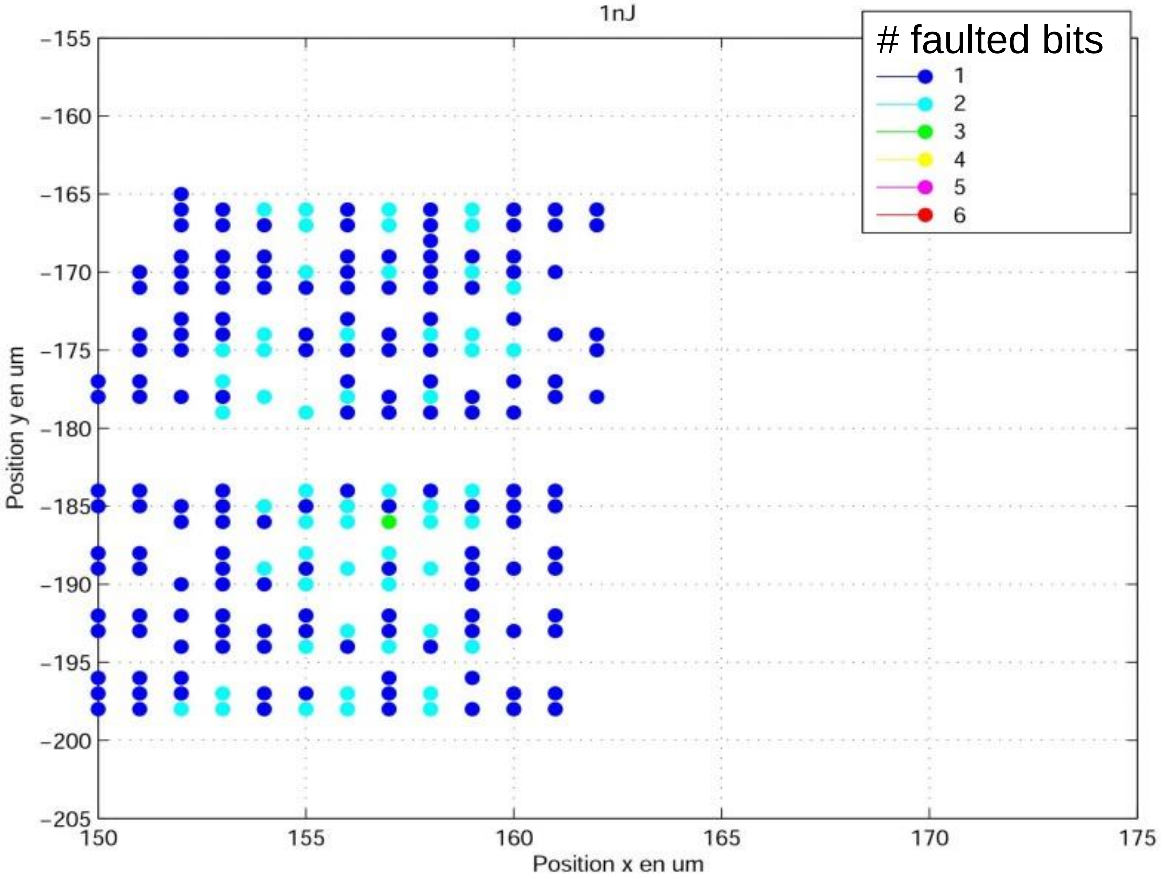
- ❑ Custom D flip-flop registers, CMOS 28 nm
  - spot 1 µm / **30 ps** / ~ 1 nJ / Δxy = 1 µm / backside



slave latch
(clk = 0)

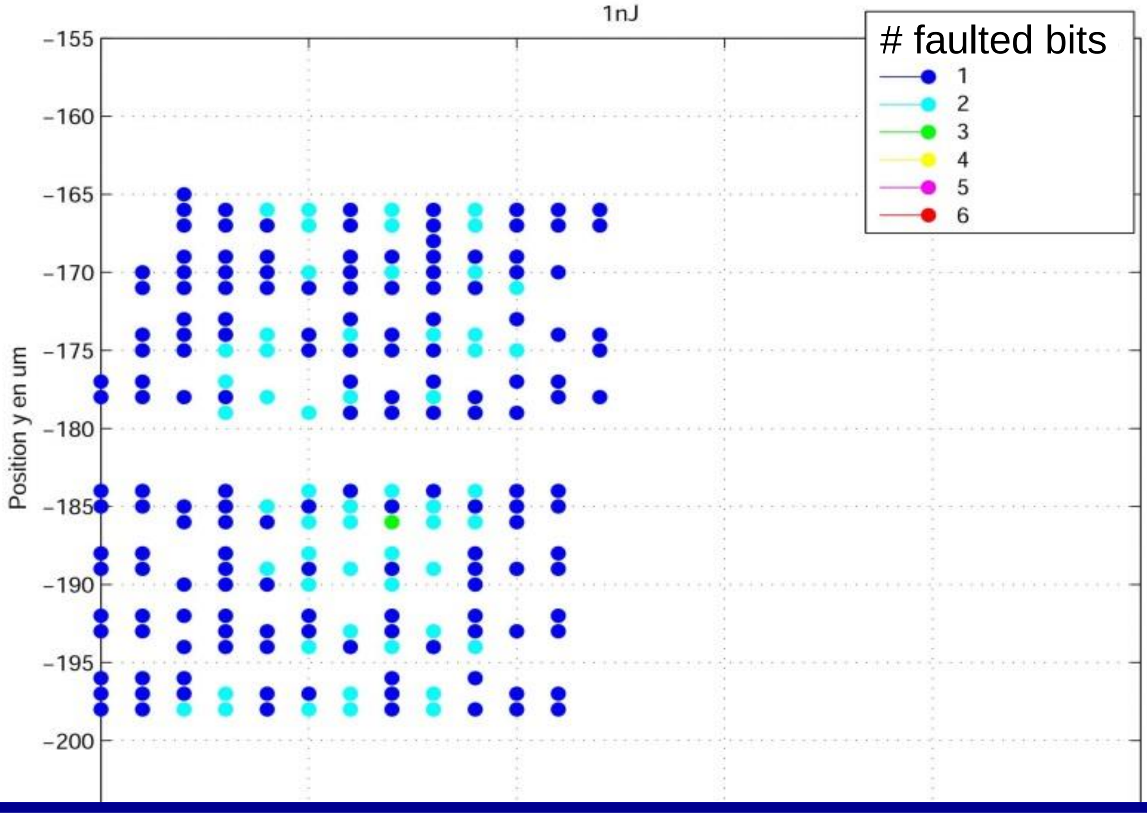
❑ Custom D flip-flop registers, CMOS 28 nm

- spot 1 µm / **30 ps** / ~ 1 nJ / ∆xy = 1 µm / backside



❑ Custom D flip-flop registers, CMOS 28 nm

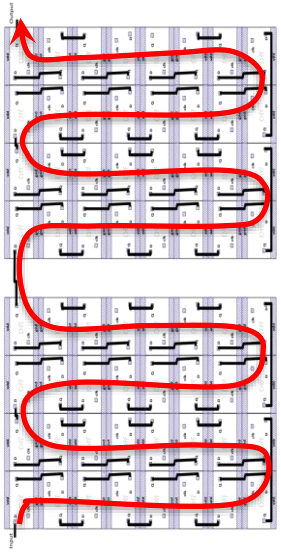
- spot 1 µm / **30 ps** / ~ 1 nJ / Δxy = 1 µm / backside

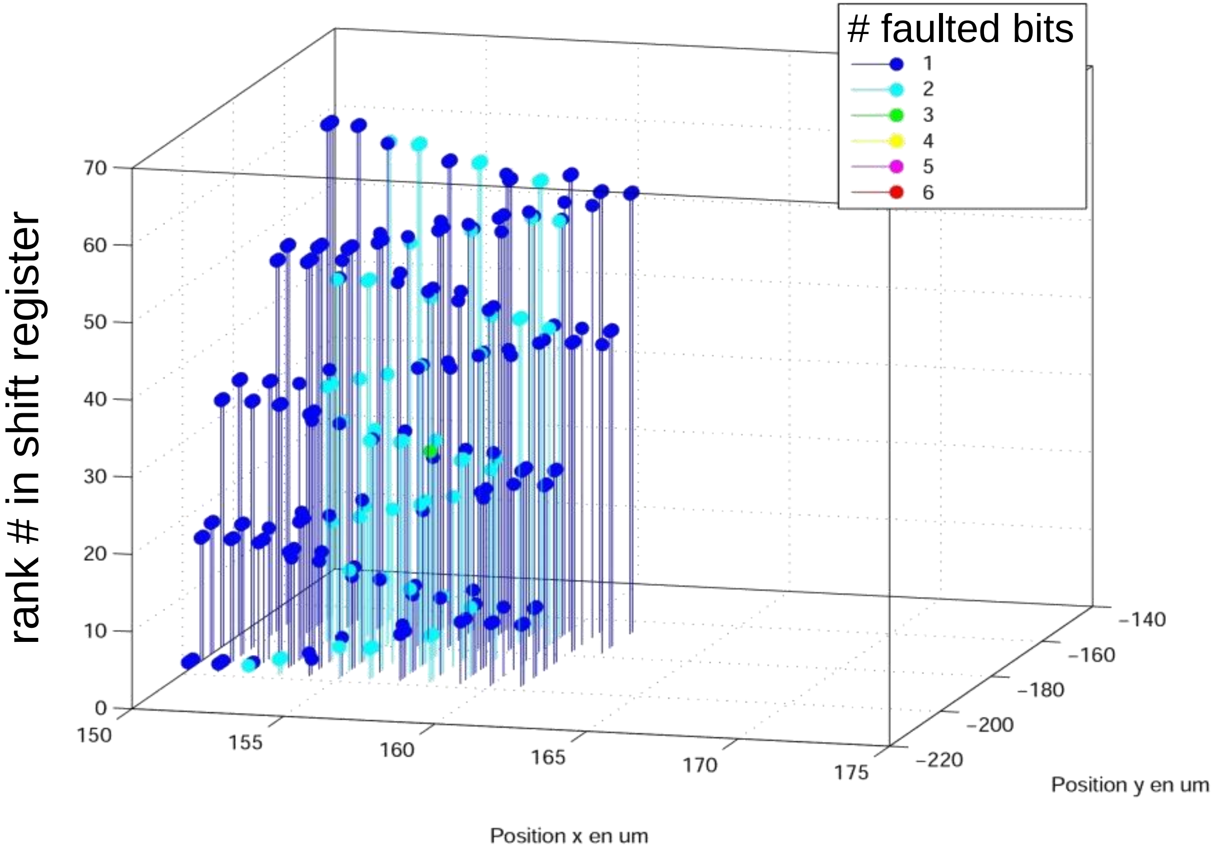


Obtained faults: **149 x 1 bit** / 62 x 2 bits / 4 x 3 bits / 1 x 20 bits

❑ Custom D flip-flop registers, CMOS 28 nm

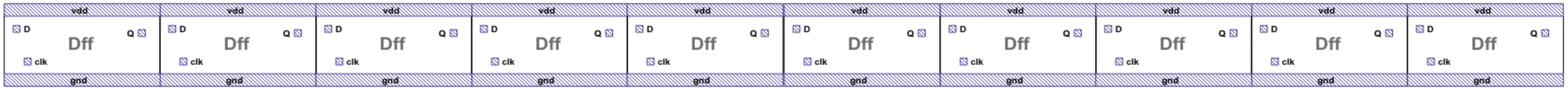
- 3D view





❑ Custom D flip-flop registers, CMOS 28 nm

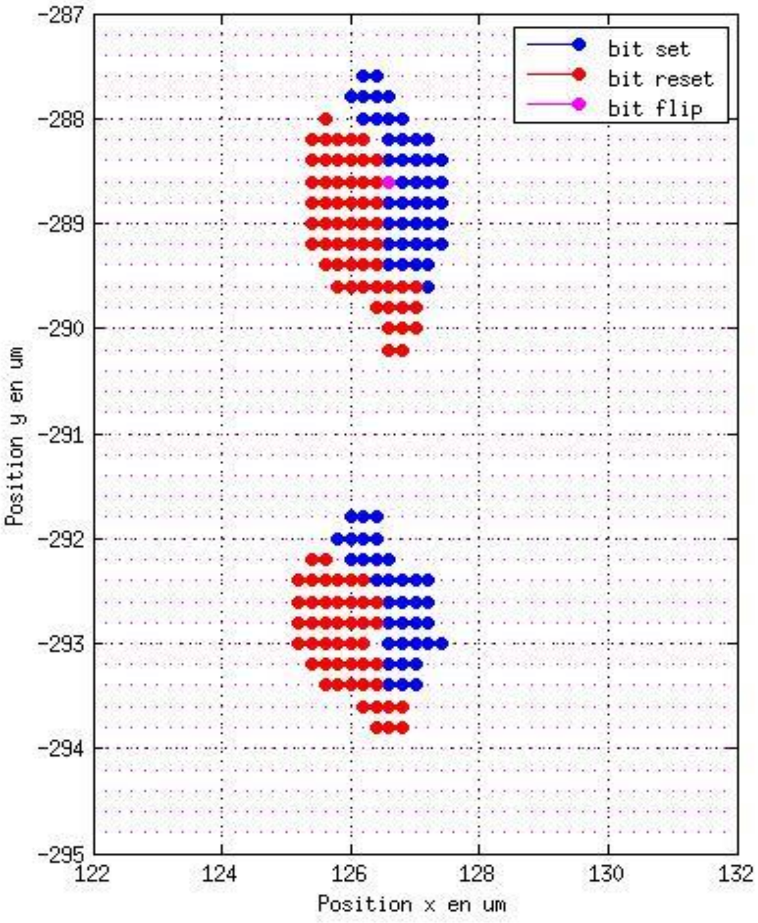
- in-line shift register with 10 D flip-flops



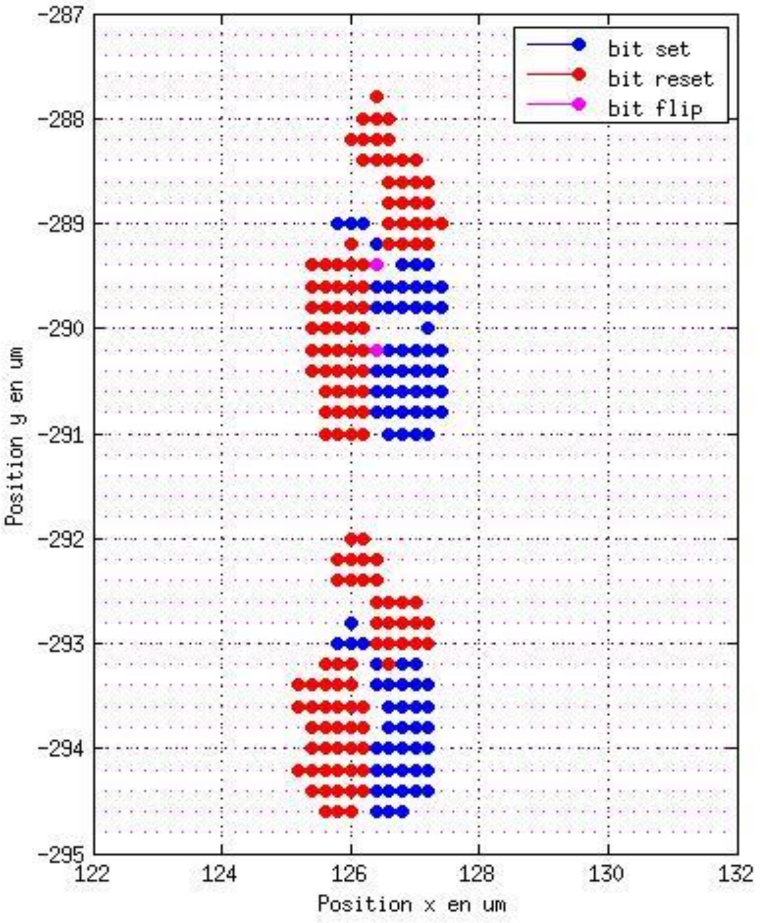
❑ Custom D flip-flop registers, CMOS 28 nm

- spot 1 µm / **30 ps** / ~ 1 nJ / Δxy = 0.2 µm / backside

clk = 0 (slave latch)



clk = 1 (master latch)



❑ Memory elements – Conclusion

Bit-set/reset fault model = relevant

Single-bit fault model experimentally assessed with a laser up to the CMOS 28 nm node.

Should be taken into account for threat evaluation.

Well defined laser-sensitive areas: implication at 14 nm?

Agenda

I. Introduction

II. Theory of laser fault injection

III. Practice of laser fault injection

Laser fault injection bench

Questions raised by technological advances

Experiment results (from CMOS 350 nm to 28 nm)

- memory elements
- microcontroller
- ASIC

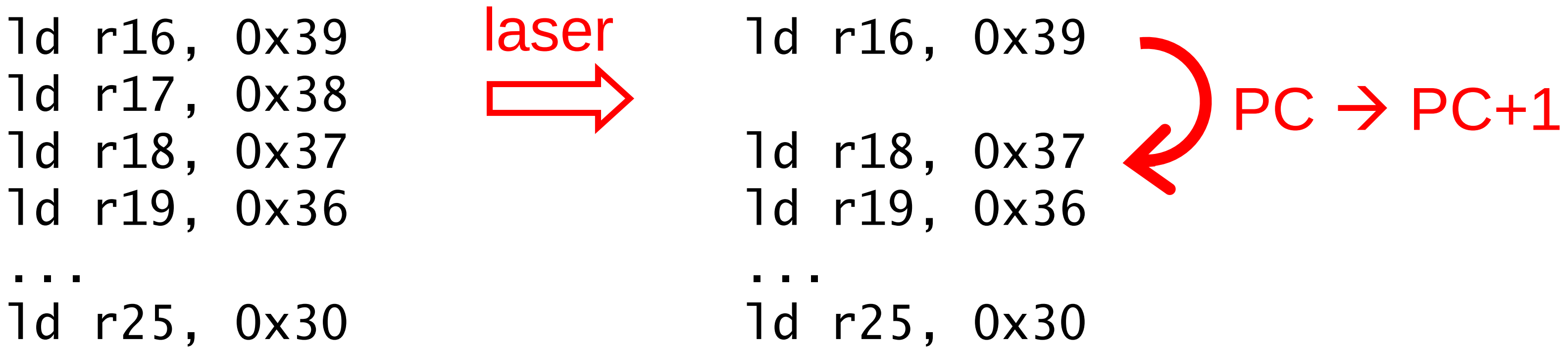
IV. Conclusion

❑ Microcontroller – ATmega328P, 8bit, 16 MHz

▪ Instruction skip fault model

Analysis of the laser instruction skip fault model:

- Program Counter increase (PC → PC + 1)?



```
ld r16, 0x39
ld r17, 0x38
ld r18, 0x37
ld r19, 0x36
...
ld r25, 0x30
```

laser

```
ld r16, 0x39

ld r18, 0x37
ld r19, 0x36
...
ld r25, 0x30
```

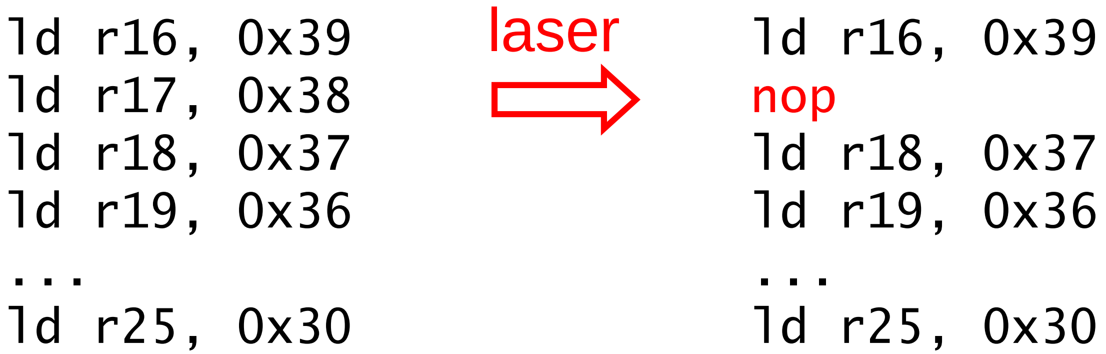
PC → PC+1

❑ Microcontroller – ATmega328P, 8bit, 16 MHz

- Instruction skip fault model

Analysis of the laser instruction skip fault model:

- Instruction alteration (no operation, nop or changed)?



```
ld r16, 0x39
ld r17, 0x38
ld r18, 0x37
ld r19, 0x36
...
ld r25, 0x30
```

laser

```
ld r16, 0x39
nop
ld r18, 0x37
ld r19, 0x36
...
ld r25, 0x30
```

Single nop

❑ Microcontroller – ATmega328P, 8bit, 16 MHz

- Instruction skip fault model

Analysis of the laser instruction skip fault model:

- Instruction alteration (no operation, nop or changed)?

```
ld r16, 0x39
ld r17, 0x38
ld r18, 0x37
ld r19, 0x36
...
ld r25, 0x30
```

laser ⇒

```
ld r16, 0x39
nop
nop
nop
...
ld r25, 0x30
```

Single nop

Several consecutive nops

❑ Microcontroller – ATmega328P, 8bit, 16 MHz

▪ Instruction skip fault model

Analysis of the laser instruction skip fault model:

- Instruction alteration (no operation, nop or changed)?

```
ld r16, 0x39
ld r17, 0x38
ld r18, 0x37
ld r19, 0x36
...
ld r25, 0x30
```

laser →

```
ld r16, 0x39
nop
ld r18, 0x37
nop
...
ld r25, 0x30
```

Single nop

Several consecutive nops

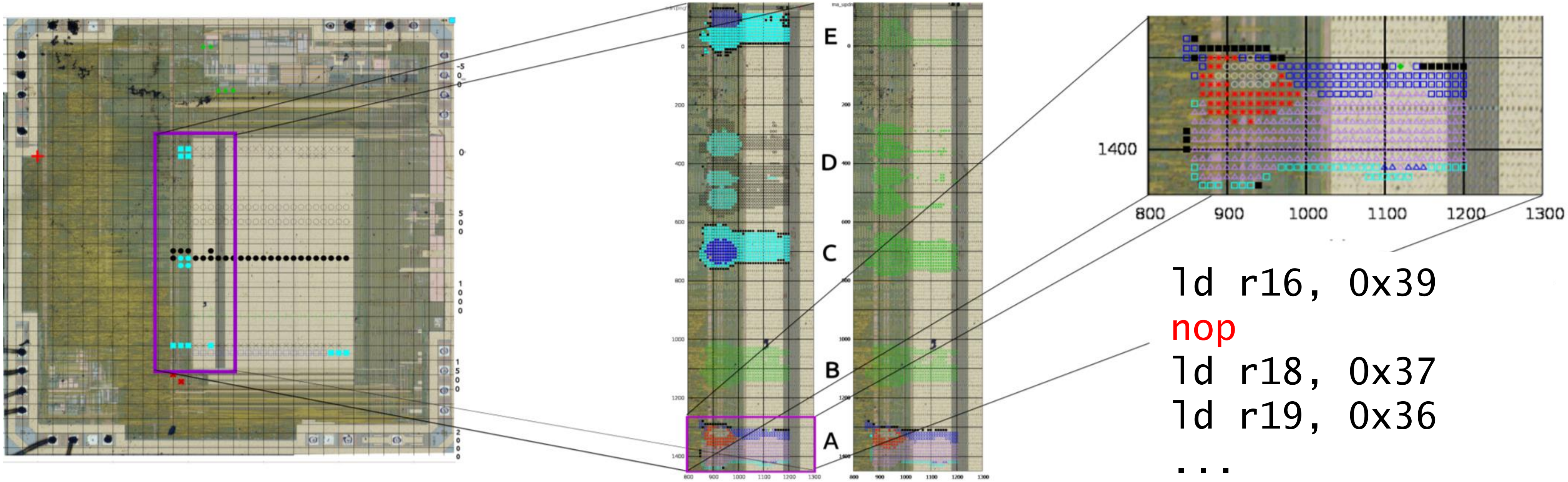
Several non-consecutive nops

T. Riom, J.-M. Dutertre, O. Potin, and J.-B. Rigaud. Practical results on laser-induced instruction- skip attacks into microcontrollers. TRUDEVICE Workshop, Barcelon Spain, 2016.

❑ Microcontroller – ATmega328P, 8bit, 16 MHz

- Instruction skip fault model

Exp. laser sensitivity map: laser 200ns, 0.4W



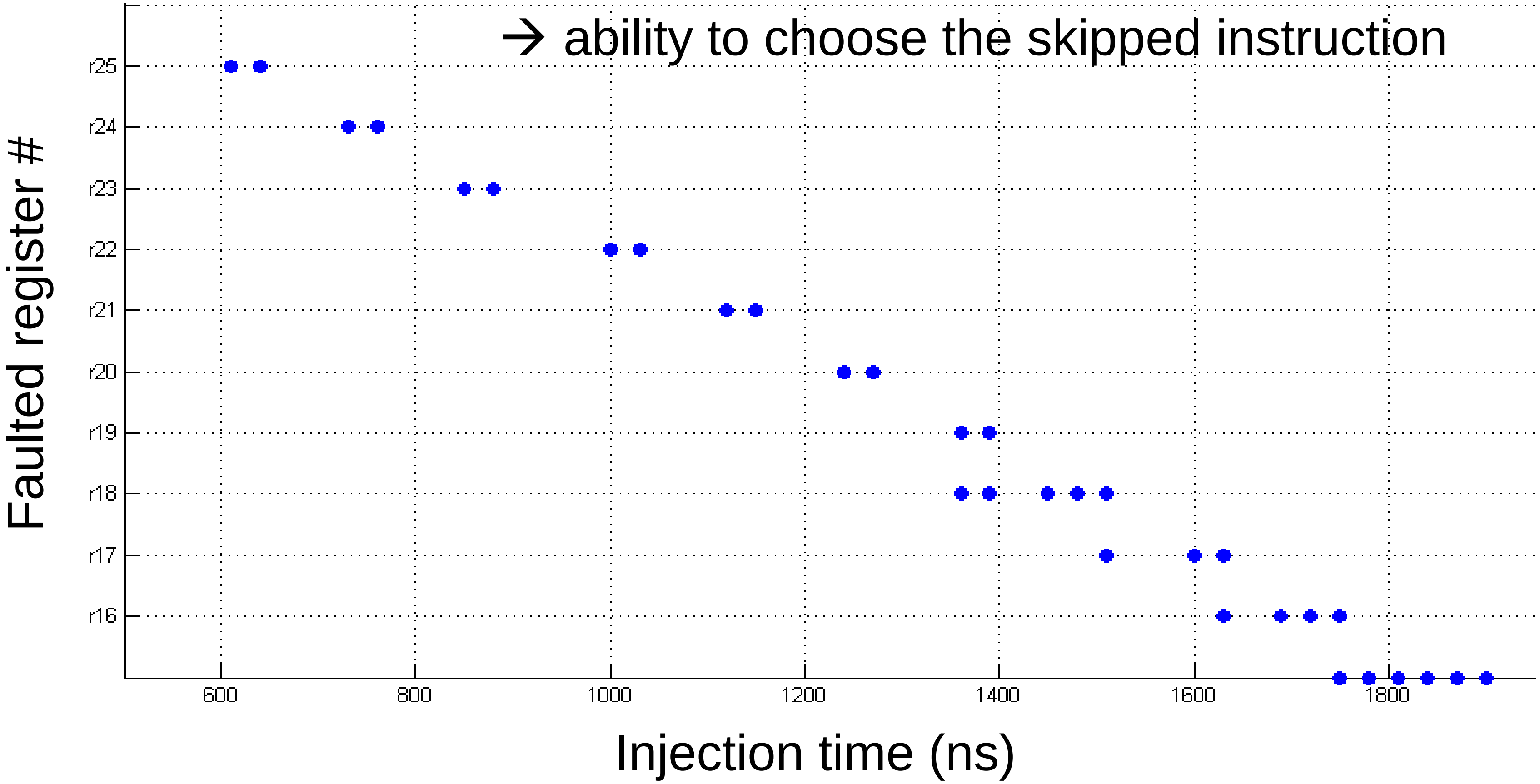
```
ld r16, 0x39
nop
ld r18, 0x37
ld r19, 0x36
...
ld r25, 0x30
```

On exp. basis: nop based laser induced instruction skip

❑ Microcontroller – ATmega328P, 8bit, 16 MHz

- Instruction skip fault model properties

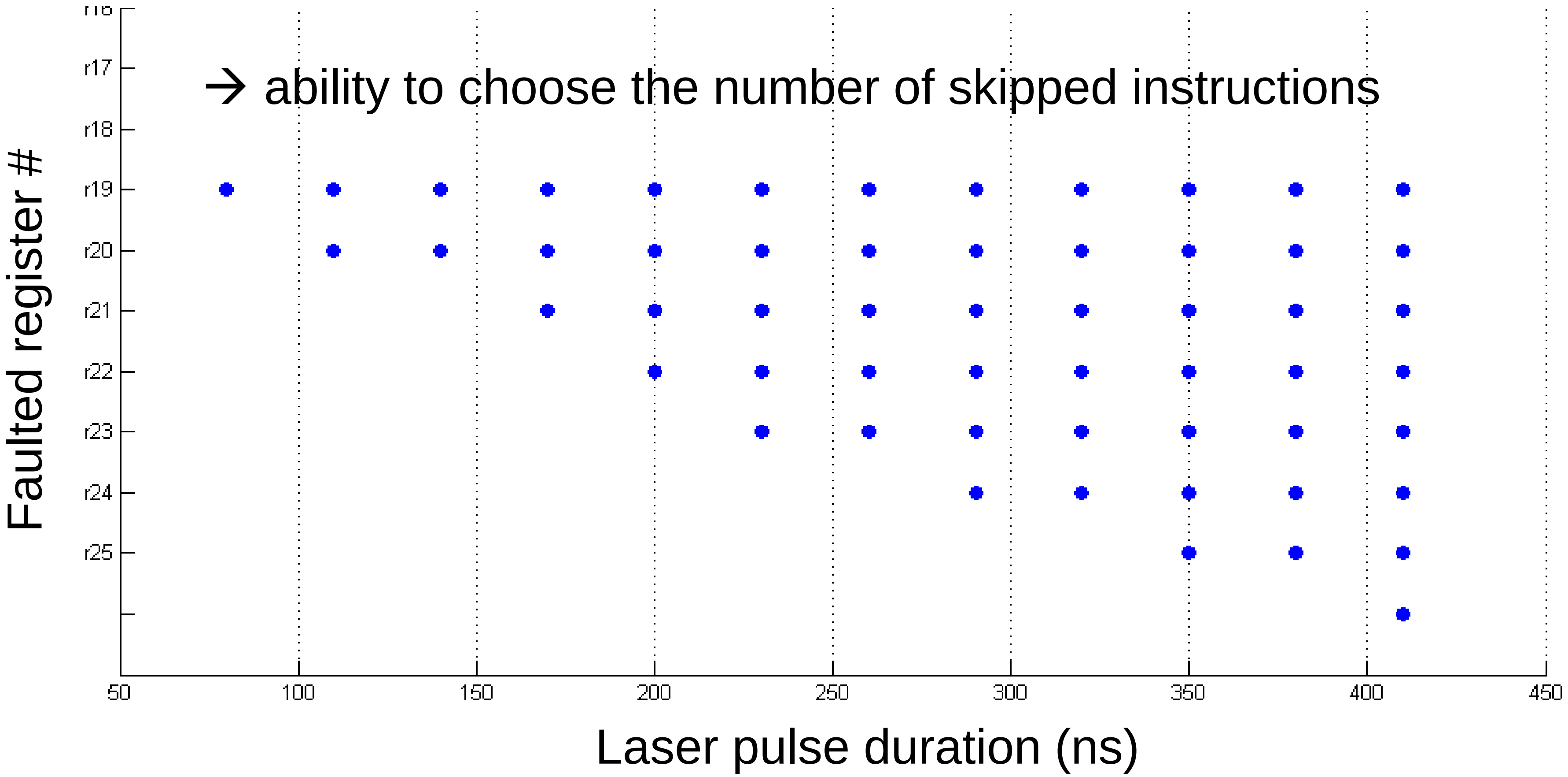
Time control (laser pulse: 75ns, 0.4W)



❑ Microcontroller – ATmega328P, 8bit, 16 MHz

- Instruction skip fault model properties

Pulse duration control (laser pulse: from 75ns, 0.4W)



→ ability to choose the number of skipped instructions

Agenda

I. Introduction

II. Theory of laser fault injection

III. Practice of laser fault injection

Laser fault injection bench

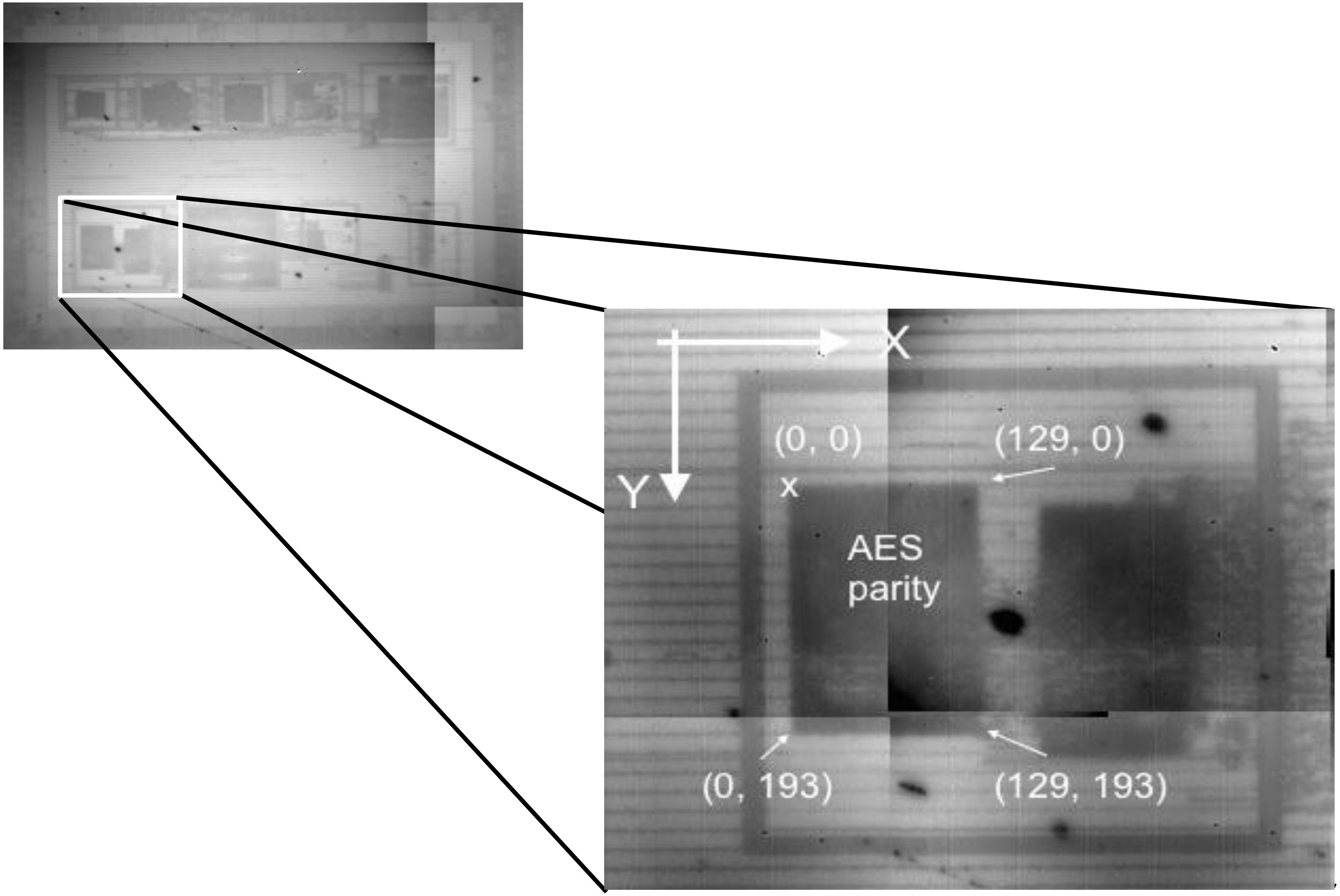
Questions raised by technological advances

Experiment results (from CMOS 350 nm to 28 nm)

- memory elements
- microcontroller
- ASIC

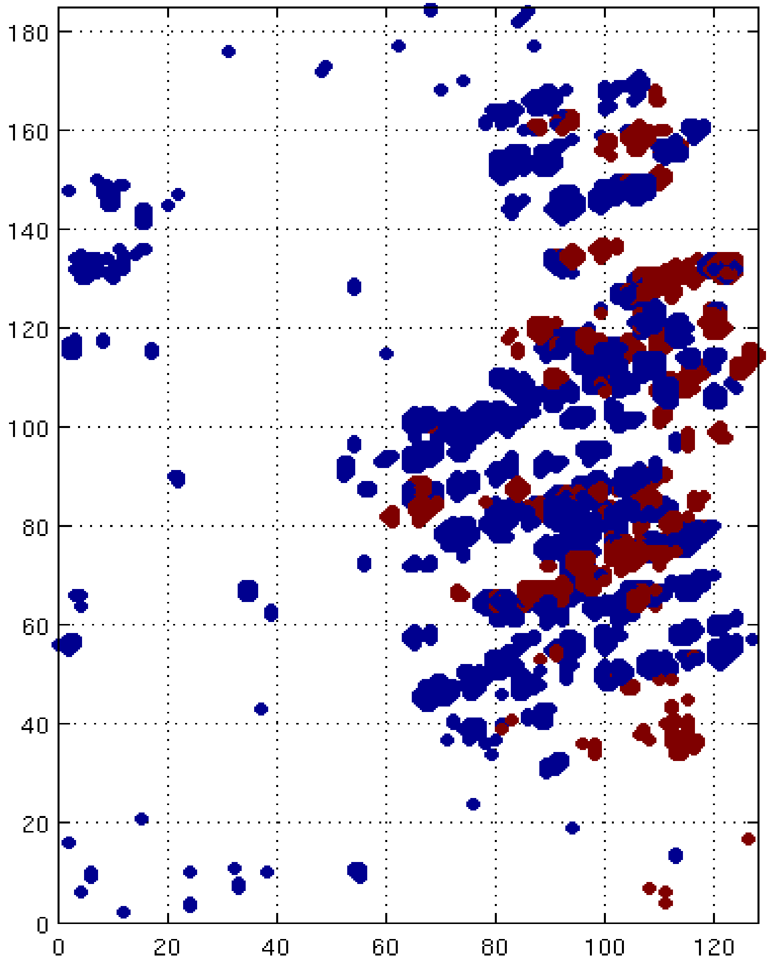
IV. Conclusion

- ASIC, crypto-accelerator
    - Hardware AES-128, CMOS 28nm, Vdd = 1.2V, 100MHz



- Hardware AES-128, CMOS 28nm, Vdd = 1.2V, 100MHz

Exp.: 5µm spot, 10ns, 0.6-1.0W, ∆xy = 1µm, Piret’s fault model



26,380 faulted cipher texts

● Unidentified faults

6,574 (24.9 %)

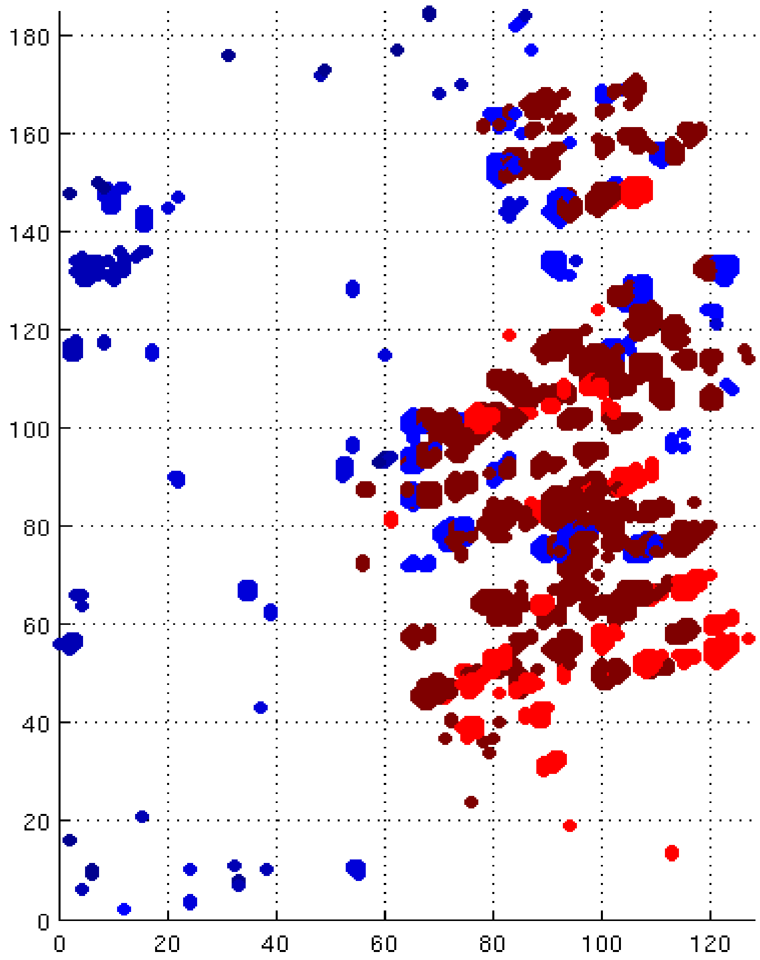
mainly 5 – 8 faulty bytes (up to12)

● Identified faults

mainly single-byte faults

- Hardware AES-128, CMOS 28nm, Vdd = 1.2V, 100MHz

  Exp.: 5µm spot, 10ns, 0.6-1.0W, Δxy = 1µm, Piret's fault model



Among the 19,806 identified faults

● key schedule (round key computation)

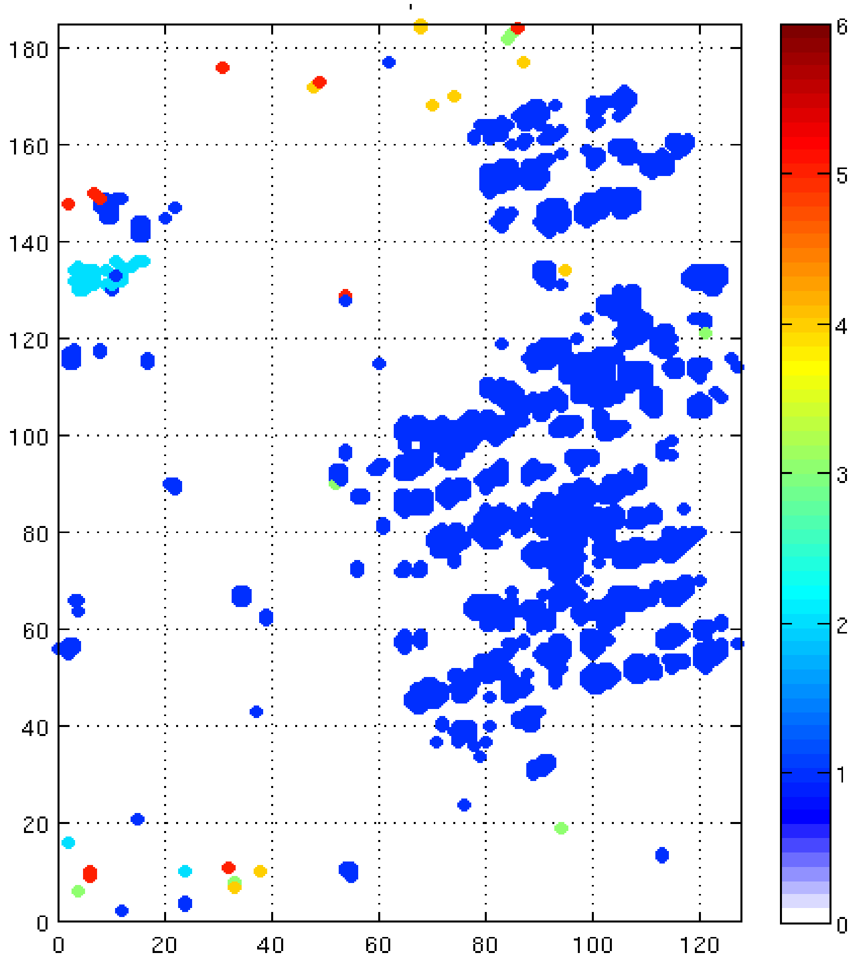
16,253 (61.6 %)

● datapath (ciphering block)

3,553 (13.5 %)

- Hardware AES-128, CMOS 28nm, Vdd = 1.2V, 100MHz

  Exp.: 5µm spot, 10ns, 0.6-1.0W, ∆xy = 1µm, Piret’s fault model



Fault model (among single-byte)

# faulted bits	Occurrence
1	19,413
2	278
3	27
4	48
5	38
6	1

Agenda

I. Introduction

- Hardware attacks

II. Theory of laser fault injection

- Physics and basics of laser fault injection
- Fault models of laser injection

III. Practice of laser fault injection

- Laser fault injection bench
- Questions raised by technological advances
- Experiment results (from CMOS 350 nm to 28 nm)

IV. Conclusion

Conclusion

Introduction to the theory of laser fault injection

Photoelectric effect → drain of OFF MOS transistors

Experimental results of laser fault injection

On various targets (µCTRL, memory cells, ASIC)

For various technology nodes: 0.35µm to 28nm CMOS

Key points: assessment of

- the single bit/byte fault model,

- the bit-set/reset fault model,

- the instruction skip (nop) fault model.

Q? at the 14nm node?

Merci de votre attention

dutertre@emse.fr

Département Systèmes et Architectures Sécurisées
Mines Saint-Etienne, Centre de Microélectronique de Provence
13541 Gardanne FRANCE

MINES
Saint-Étienne
Une école de l'IMT

Institut Mines-Télécom