FDTC 2018
Fault Diagnosis and
Tolerance in Cryptography

FDTC 2018

# Laser Fault Injection at the CMOS 28 nm Technology Node: an Analysis of the Fault Model

J.M. Dutertre[1], V. Beroulle[2], P. Candelier[3], S. De Castro[1,4], L.B. Faber[3], M.L. Flottes[4], P. Gendrier[3], D. Hély[2], R. Leveugle[5], P. Maistri[5], G. Di Natale[4], A. Papadimitriou[2], B. Rouzeyre[4]

Amsterdam, The Netherlands — Thursday, September 13, 2018

(1) MINES Saint-Étienne
Une école de l'IMT

(2) Lcis

(3) ST life.augmented

(4) LIRMM

(5) TIMA CNRS - Grenoble INP - UGA

## ❑ A brief history of 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 scale down of CMOS technology

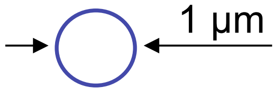
Secure devices: CMOS 40 nm

SoC: CMOS 14 nm

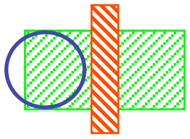
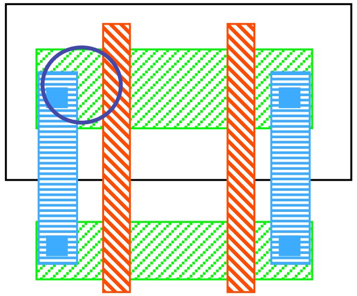
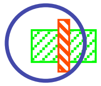
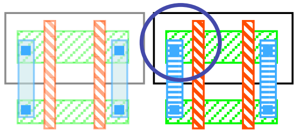
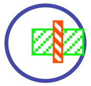
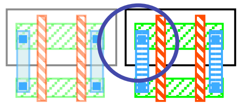
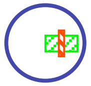
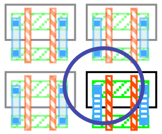
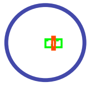
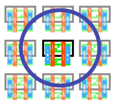
Several logic gates under a laser beam (1 µm)

# Position of the problem

## ❑ LFI accuracy vs. CMOS scale down

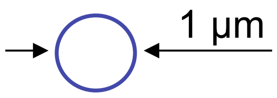


Laser spot

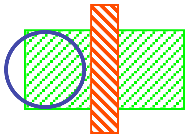
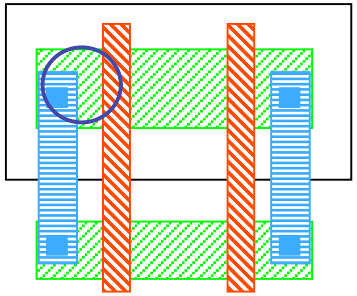
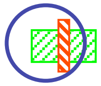
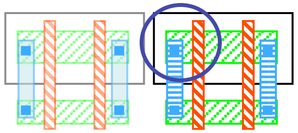
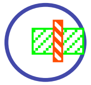
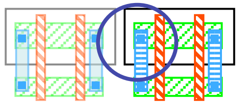
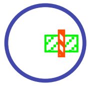
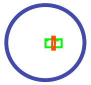
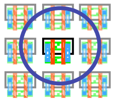
| Technology | MOS transistor | SRAM |
|---|---|---|
| 0.35 µm |  |  |
| 130 nm |  |  |
| 90 nm |  |  |
| 65 nm |  |  |
| 28 nm |  |  |

# Position of the problem

## ❑ LFI accuracy vs. CMOS scale down



Laser spot

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

Simultaneous flip of several SRAMs?

## Importance of the fault model

LFI considered as an accurate fault injection technique:

- physical location (gates under/close to the laser spot),
- injection time (regarding the course of an algorithm),
- nb. of faulted bits/bytes,
- additional information leakage (data dependence).

Makes it possible to meet the (sometimes strong) requirements of FA and DFA schemes.

Does CMOS technology scale down reduce the accuracy of the laser fault injection fault model?

# This talk

## ❑ Fault model of LFI at the CMOS 28 nm tech. node

On an experimental basis (custom test chip)

- Single-bit/single-byte fault model
- Data dependence: bit-flip vs bit-set/reset fault model
- Static LFI on D flip-flops
- Dynamic LFI on an AES encryption unit

# Agenda

I. Introduction

II. Theory of laser fault injection

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

III. Static LFI experimental results

- Setup, results, analysis

IV. Dynamic LFI experimental results

- Setup, results, analysis

V. Conclusion

# Agenda

I. Introduction

II. Theory of laser fault injection

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

III. Static LFI experimental results

- Setup, results, analysis

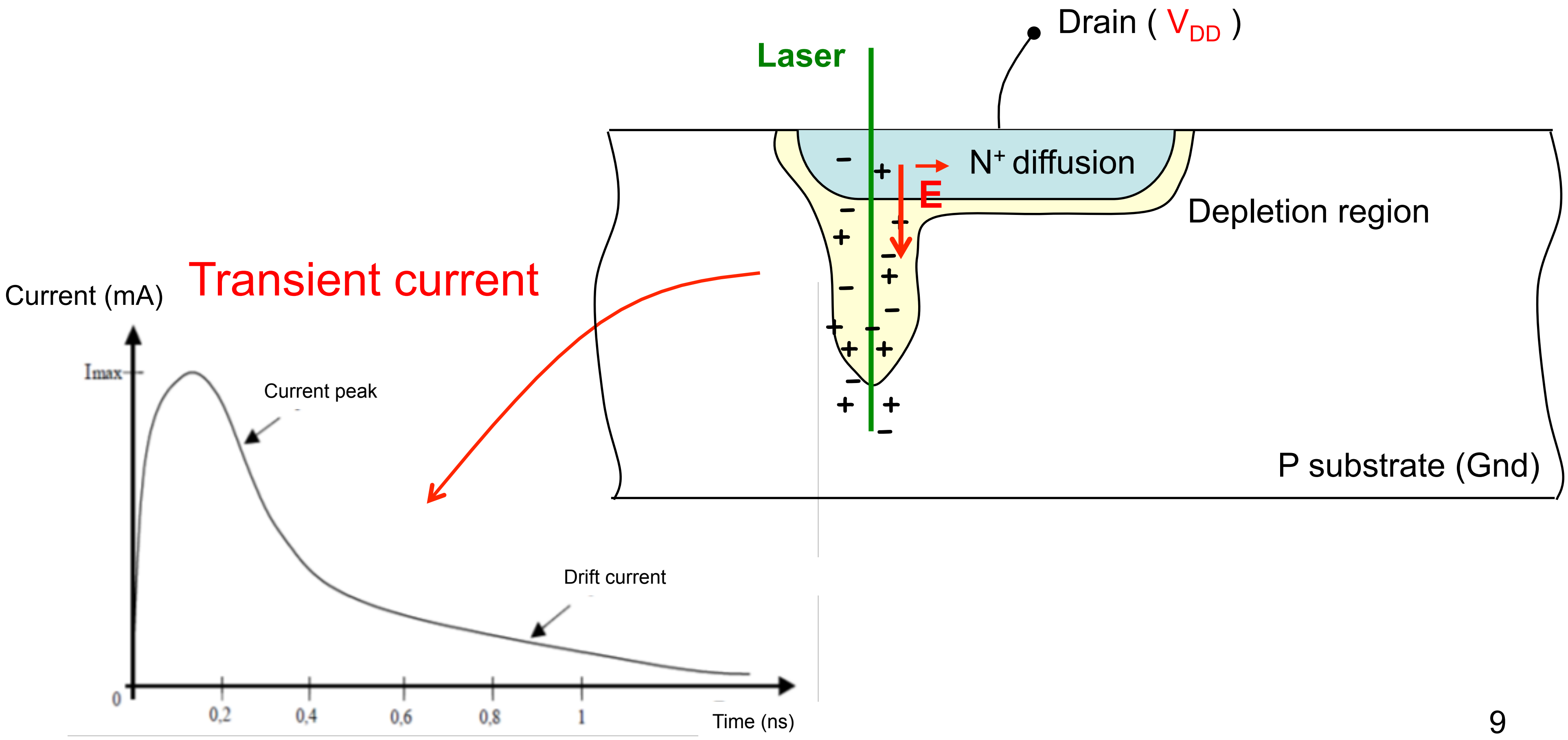
IV. Dynamic LFI experimental results

- Setup, results, analysis

V. Conclusion

## ❑ Physics of laser fault injection

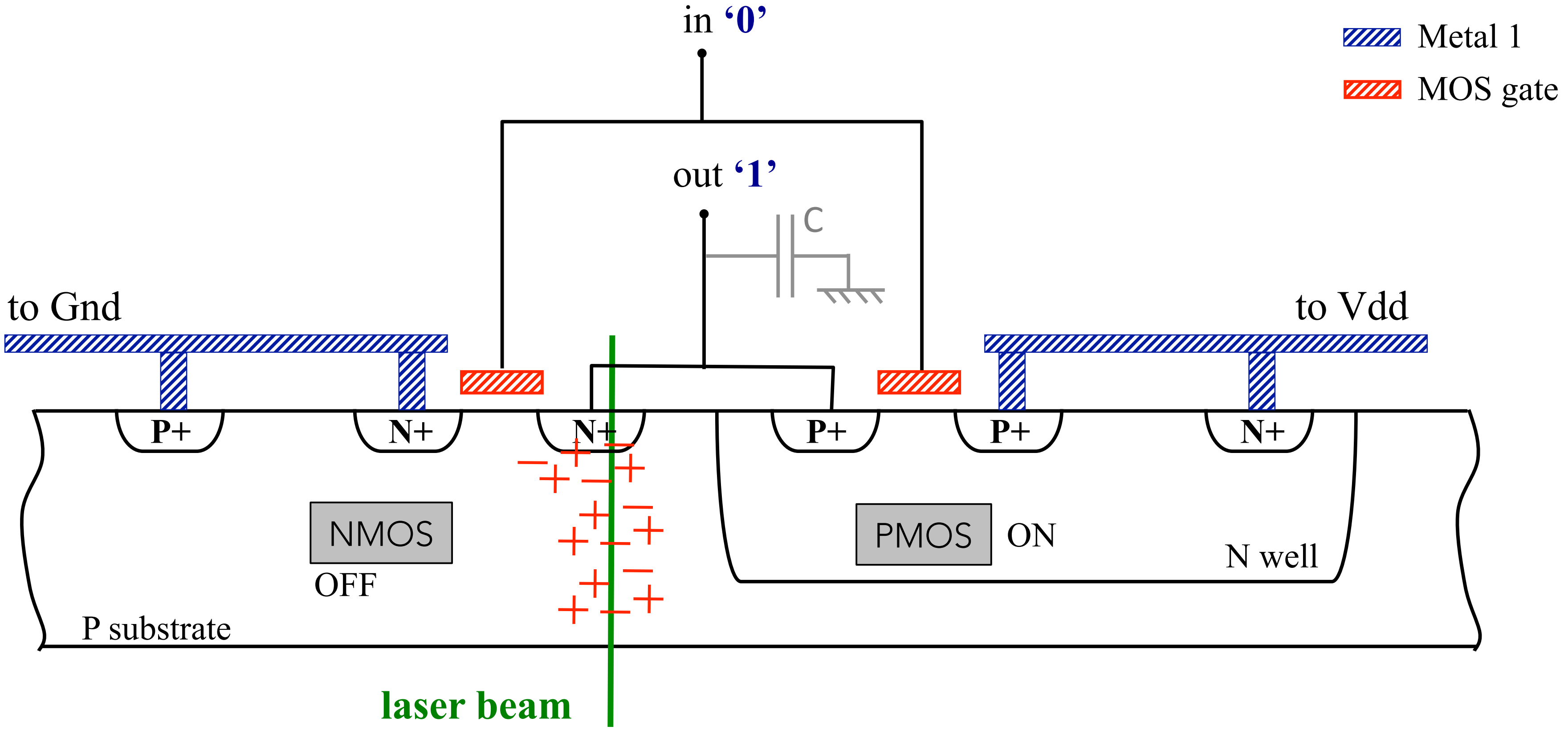
- Photoelectric effect: from a laser pulse to transient current generation (in reverse biased PN junction)



## II. Theory of laser fault injection

- Fault injection mechanism (the inverter case)

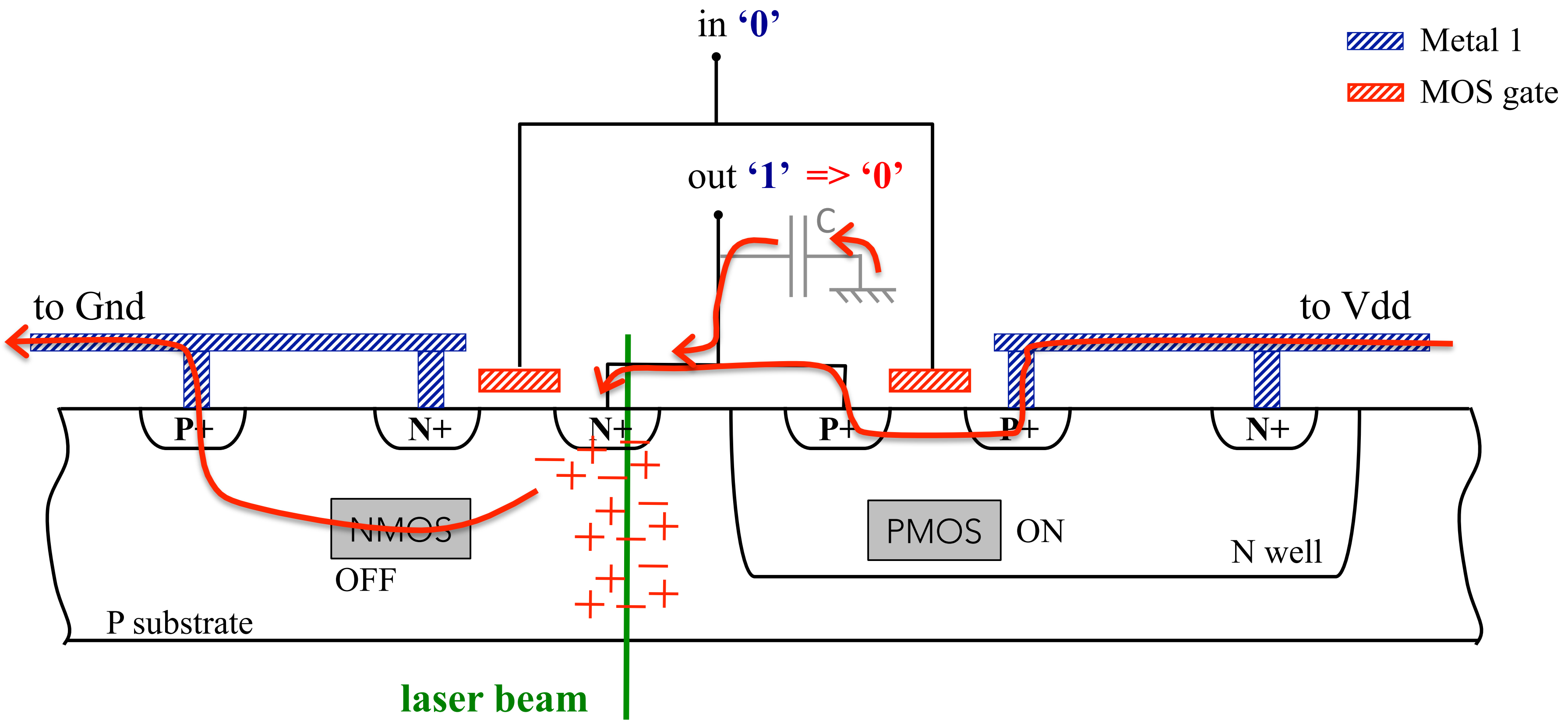
  from a transient current to a voltage transient (a.k.a. SET, single event transient)



# II. Theory of laser fault injection

- Fault injection mechanism (the inverter case)

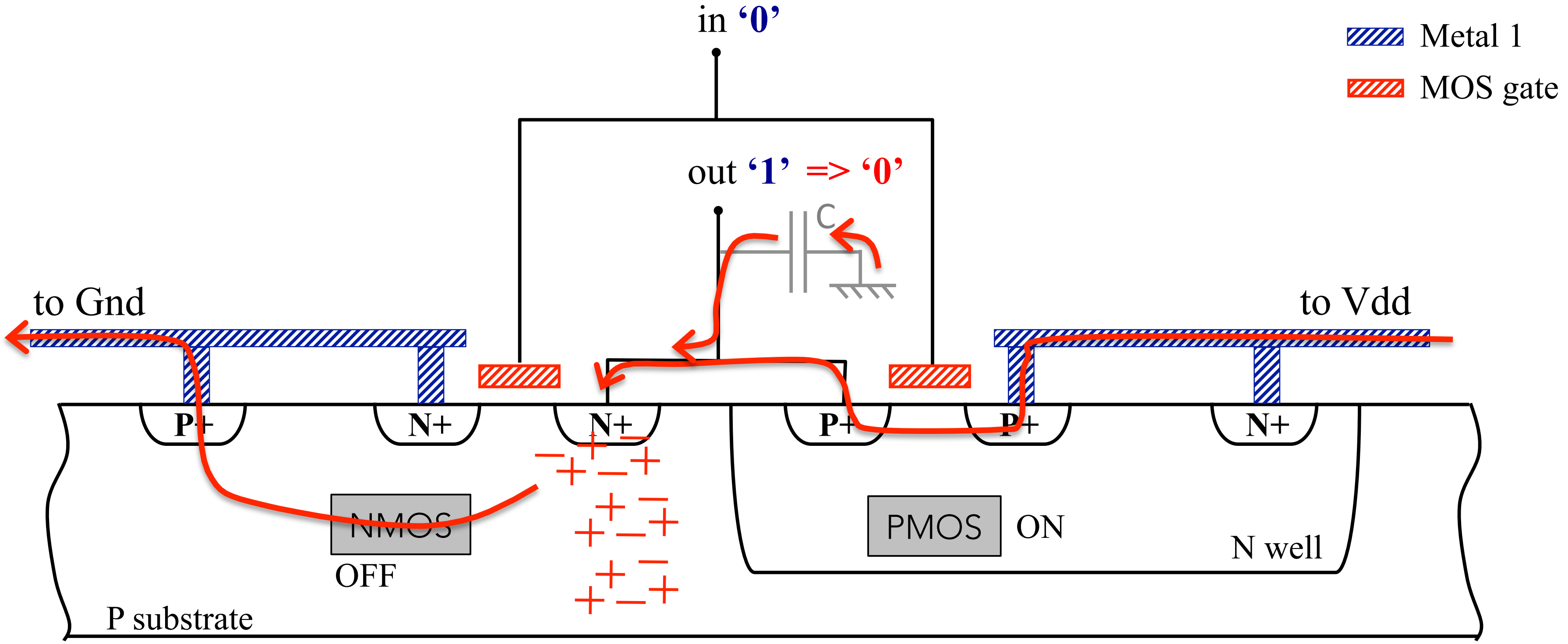
  from a transient current to a voltage transient (a.k.a. SET, single event transient)



## II. Theory of laser fault injection

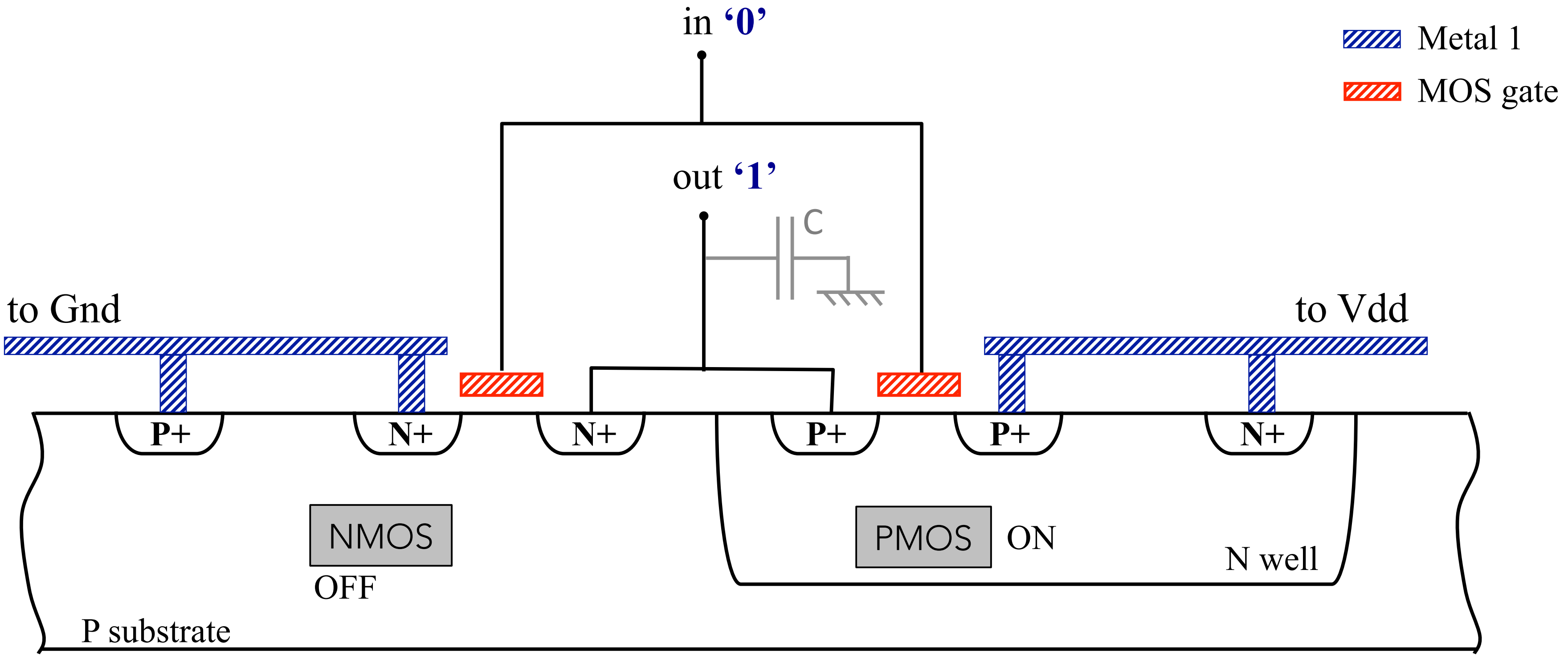
- Fault injection mechanism (the inverter case)

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



- 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

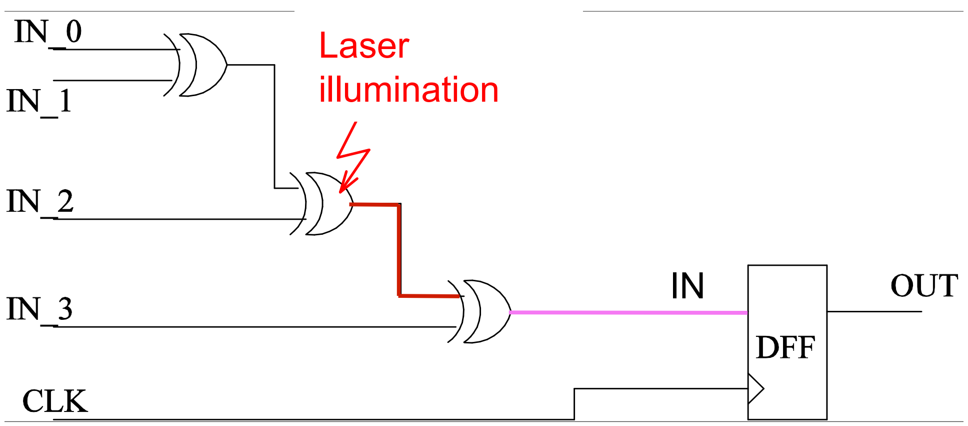
  Two mechanisms depending on the voltage transient location:

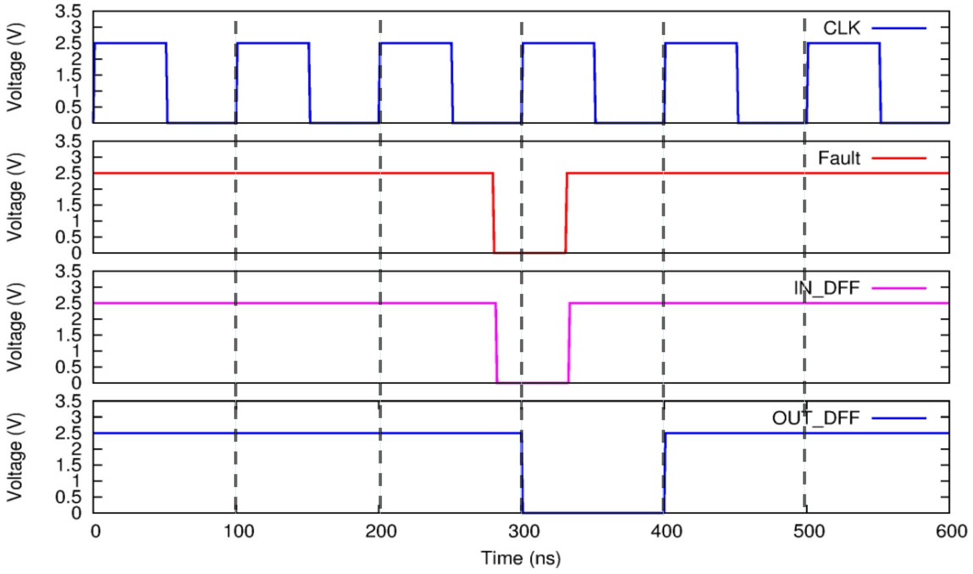
  1. logic,
  2. memory element (D flip-flop, SRAM)

# II. Theory of laser fault injection

- Fault injection mechanism – target: combinatorial logic

  from voltage transient to fault

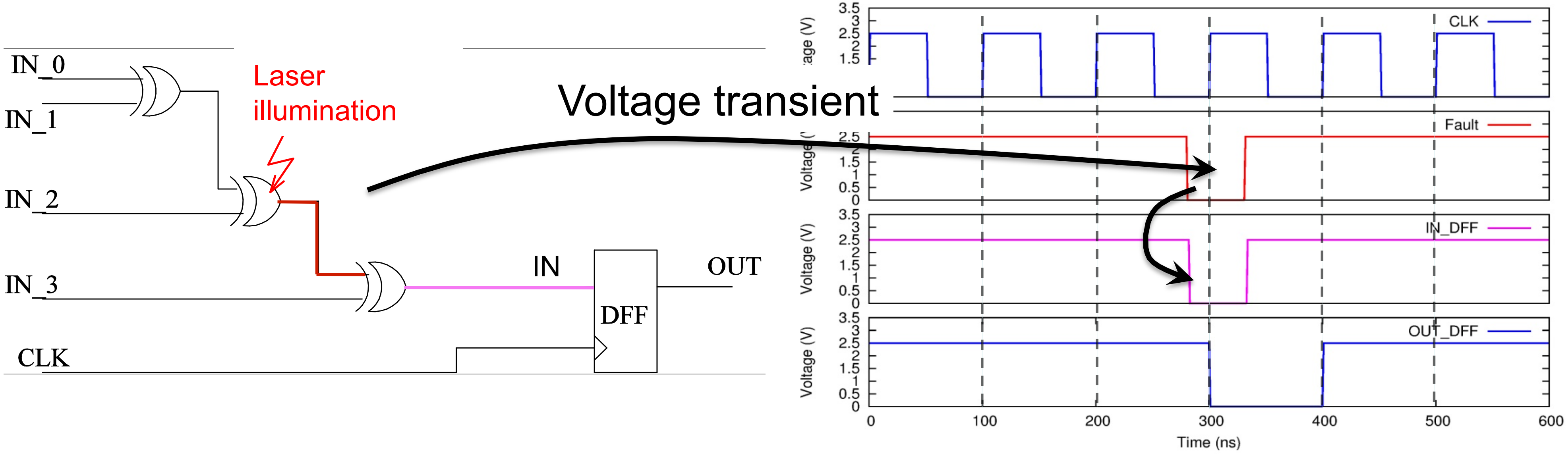




# II. Theory of laser fault injection

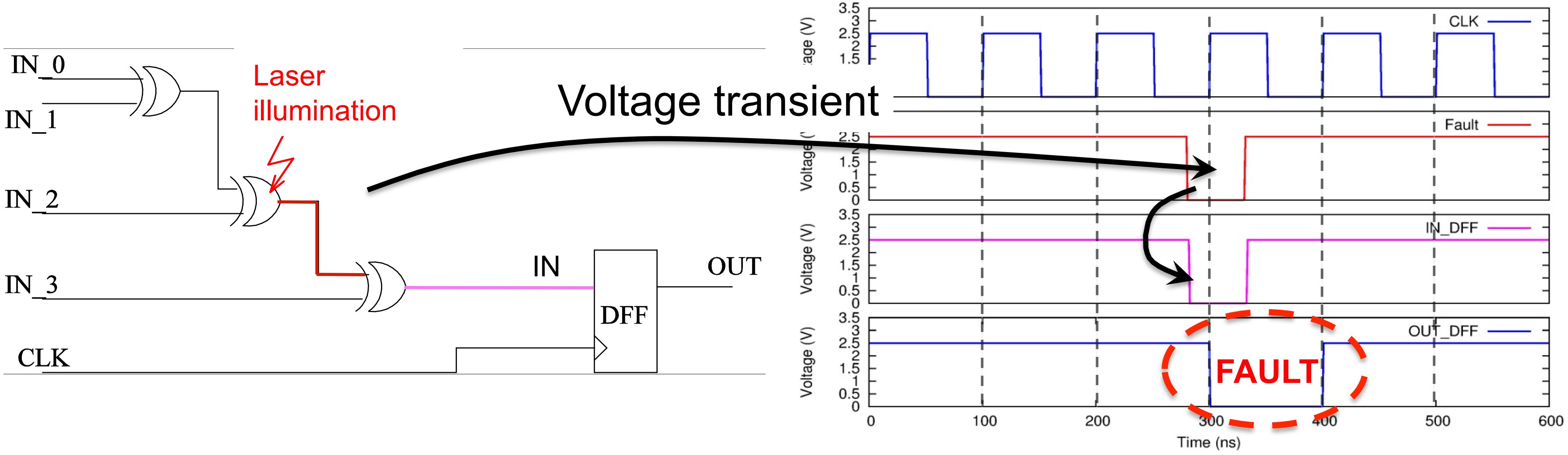
- Fault injection mechanism – target: combinatorial logic

  from voltage transient to fault



- Fault injection mechanism – target: combinatorial logic

  from voltage transient to fault

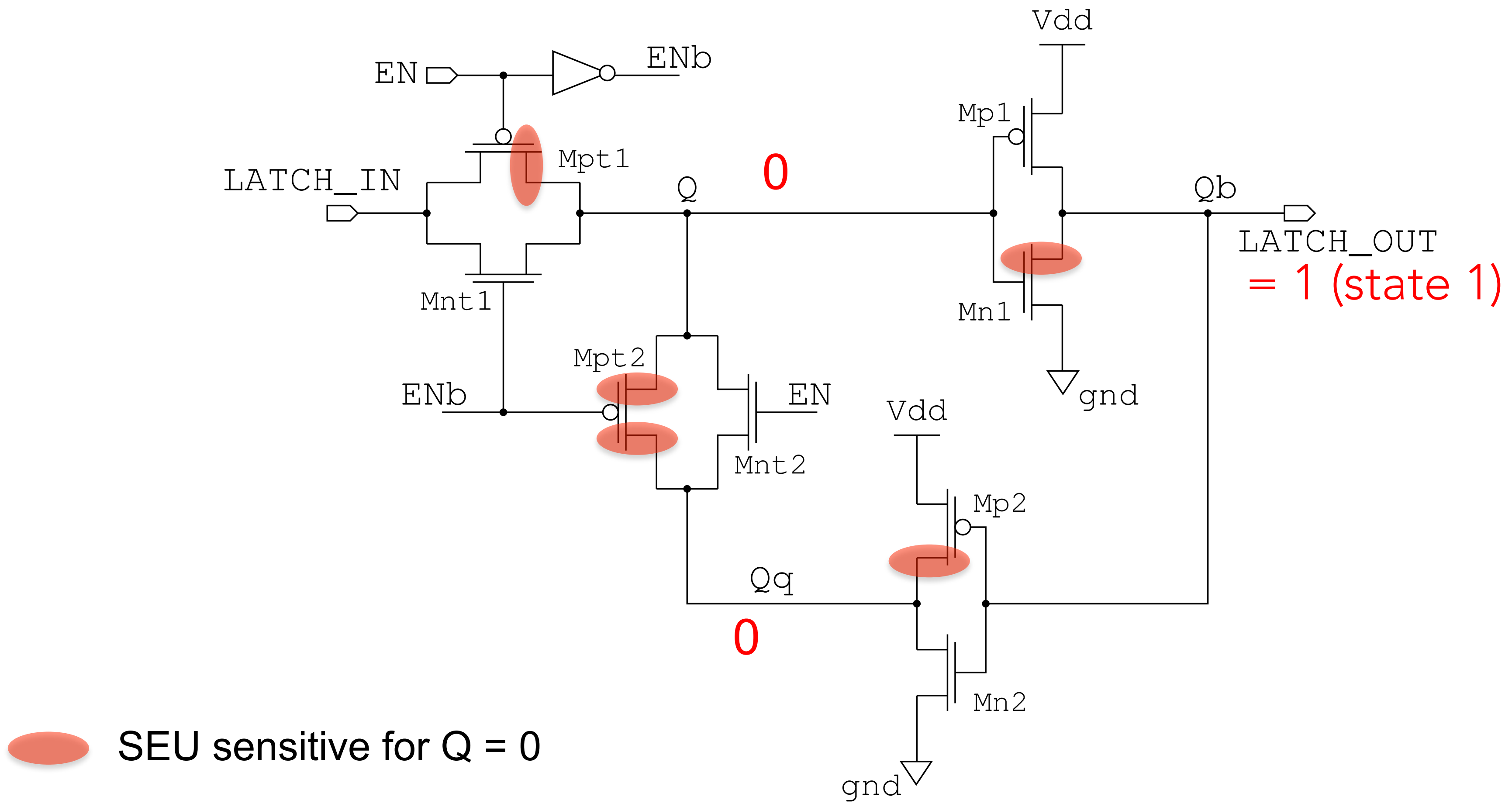


The fault injection process depends both on:

- the injection time,
- the voltage transient duration.

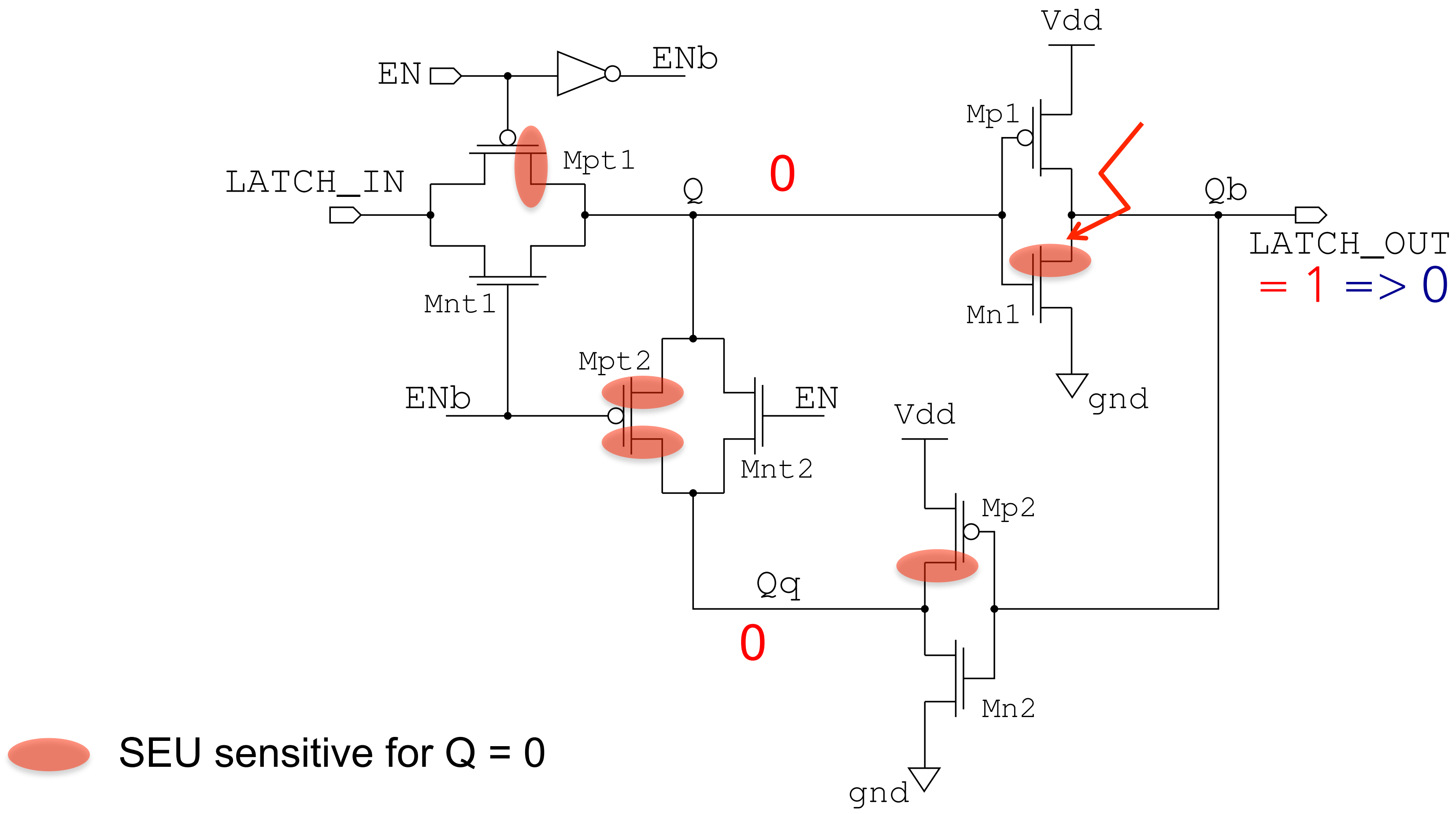
- Fault injection mechanism – target: D latch

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



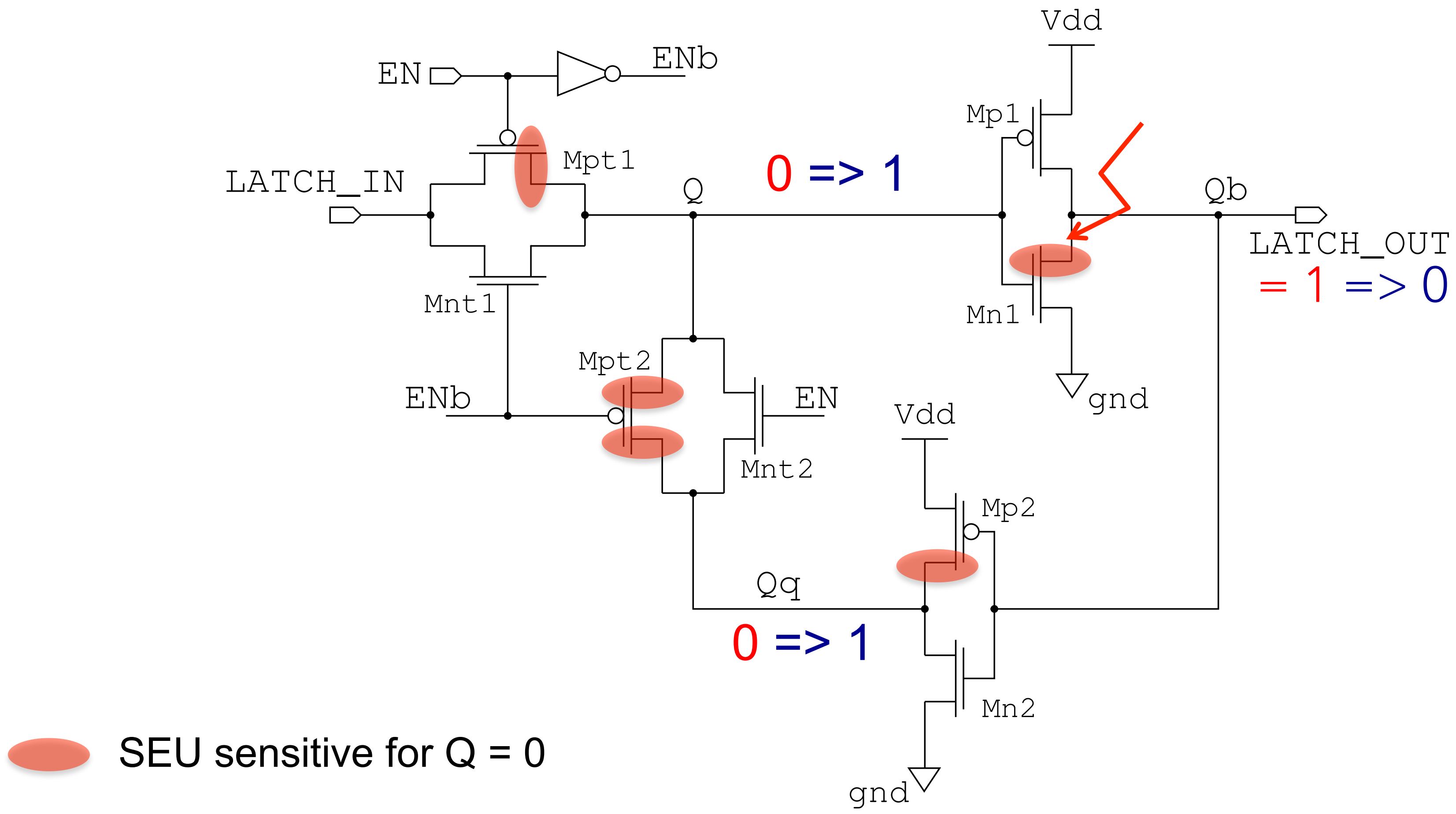
- Fault injection mechanism – target: D latch

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



- Fault injection mechanism – target: D latch

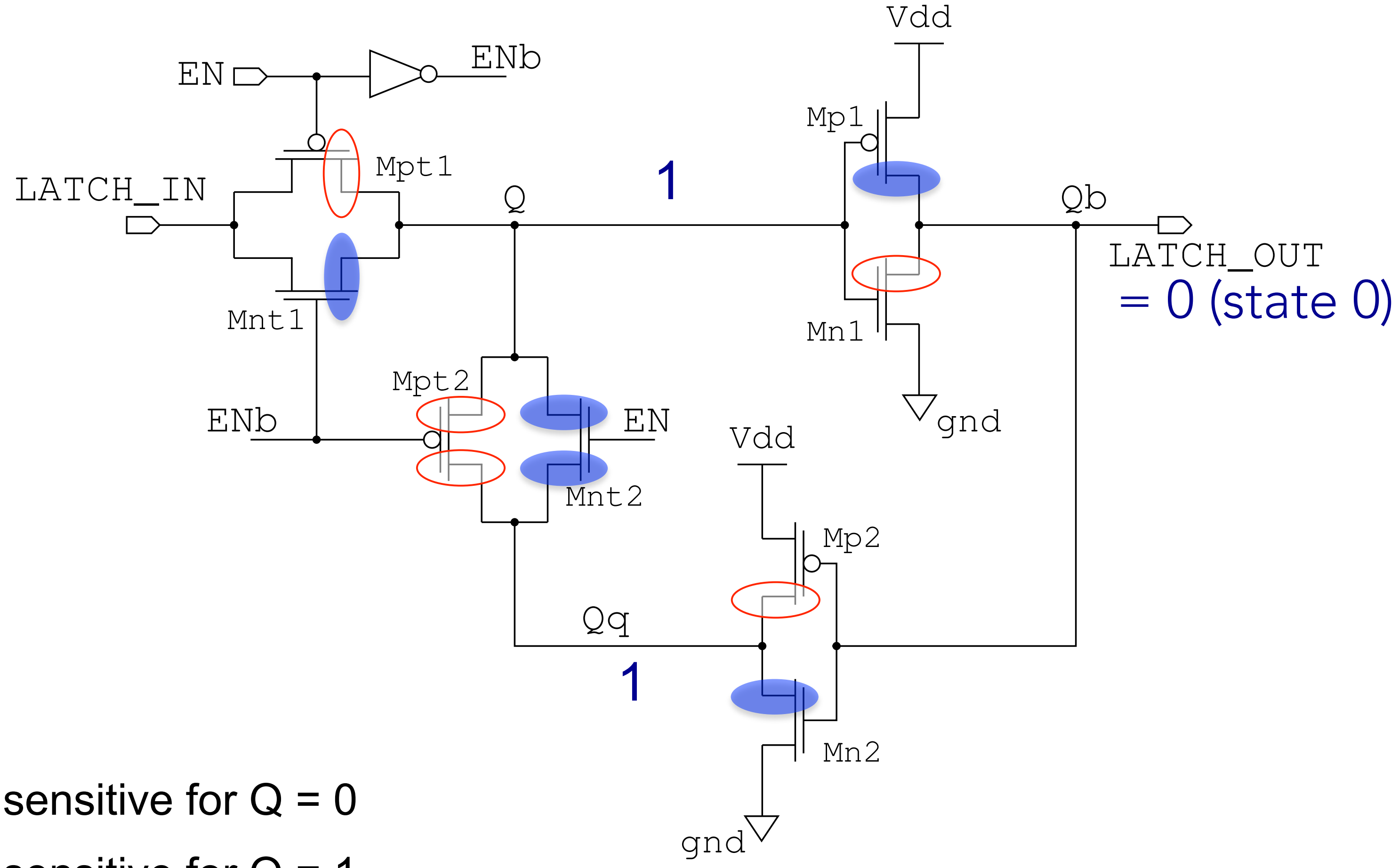
  from voltage transient to fault (SEU: single event upset)



# II. Theory of laser fault injection

- Fault injection mechanism – target: D latch

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



○ SEU sensitive for Q = 0

● SEU sensitive for Q = 1

Note the data dependence of the laser sensitive areas.

# Agenda

I. Introduction

II. Theory of laser fault injection

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

III. Static LFI experimental results

- Setup, results, analysis

IV. Dynamic LFI experimental results

- Setup, results, analysis

V. Conclusion

## ❑ Fault model: mathematical expression at bit level

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

$$b \rightarrow \quad not(b)$$

## ❑ Fault model: mathematical expression at bit level

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

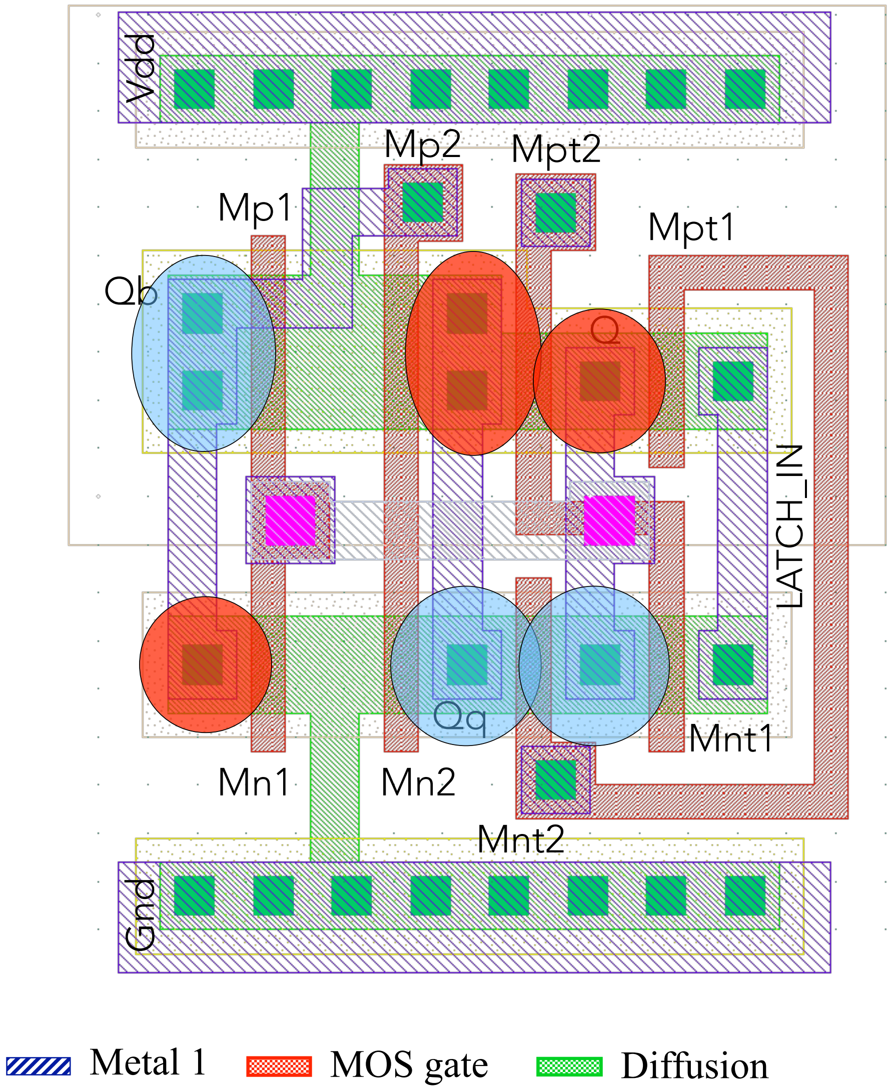
$$\left.\begin{array}{l} if \;\; b = 0 \rightarrow \;\; \boxed{b = 1} \\ if \;\; b = 1 \rightarrow \;\; b = 1 \end{array}\right\} \text{bit-set}$$

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

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

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

- bit-set/reset fault model: D latch layout vs. laser effect area

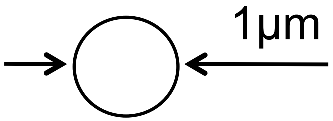


Laser sensitive areas:

🔵 SEU sensitive for Q = 1

🔴 SEU sensitive for Q = 0

Laser spot size/effect area:

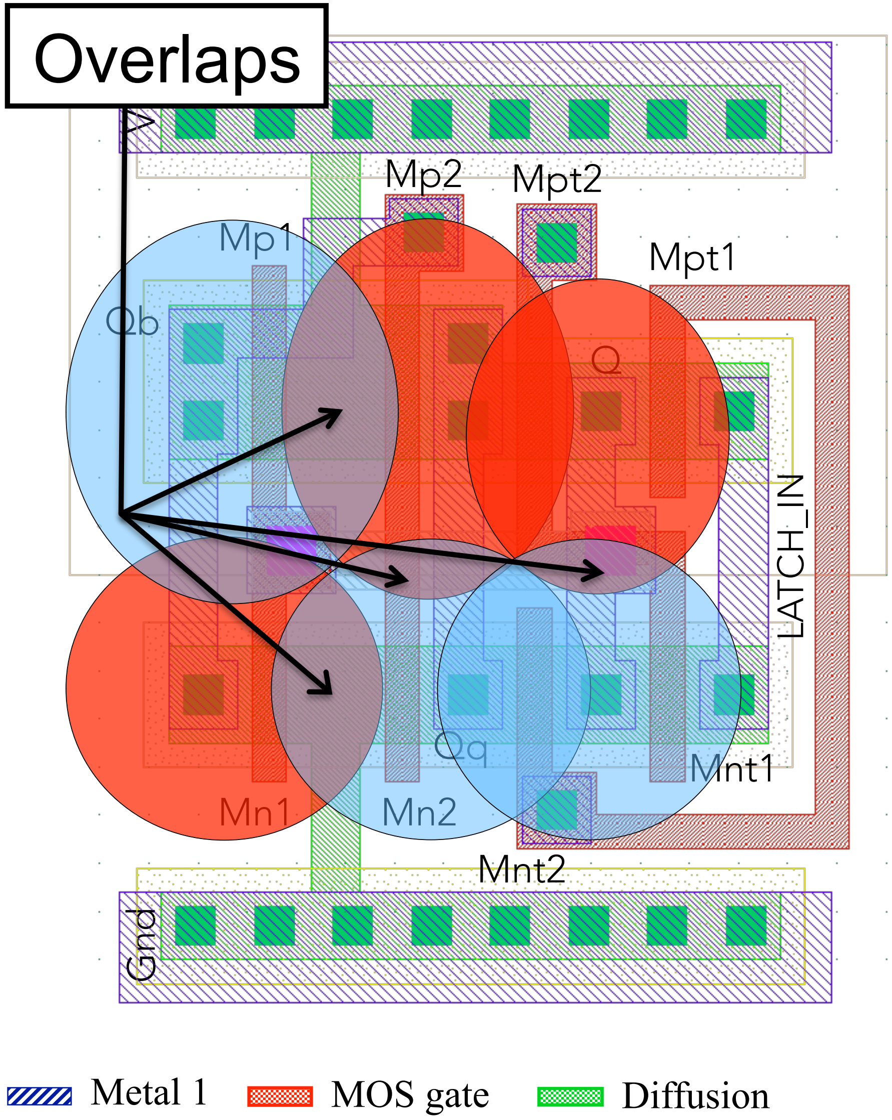


One laser sensitive area exposed

⇨ bit-set/reset fault model

# II. Theory of laser fault injection

- bit-set/reset fault model: Dff layout vs. laser effect area

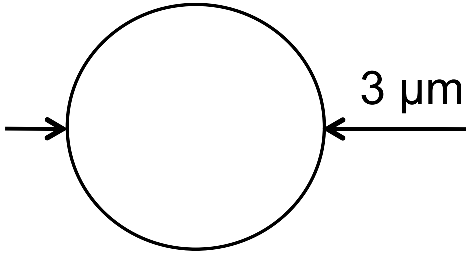


Laser sensitive areas:

🔵 SEU sensitive for Q = 1

🔴 SEU sensitive for Q = 0

Laser spot size/effect area:



Overlaps of laser sensitive areas

⇨ bit-flip fault model

## ❑ Experimental state of the art

- 2015, B. Selmke et al.: 45 nm SRAM (FPGA)
- 2015, C. Champeix et al.: 40 nm D flip-flop
- Both consistent with single-bit and bit-set/reset fault models

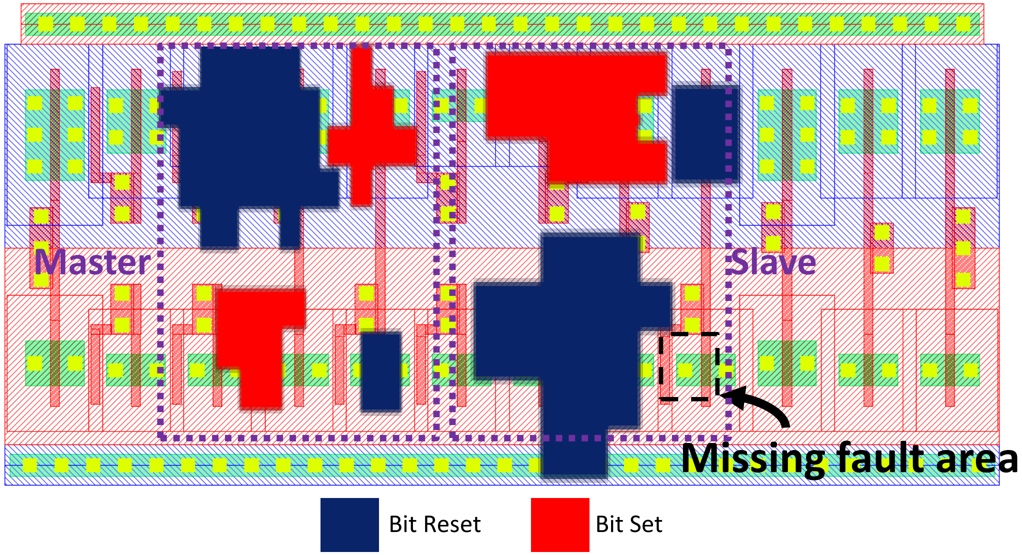


Illustration for D flip-flop:

- 4 SEU sensitive areas of master latch (clk = 1),

- 3 SEU sensitive areas of slave latch (clk = 0).

B. Selmke et al., “Precise laser fault injections into 90 nm and 45 nm sram-cells,” CARDIS 2015.

C. Champeix et al., “SEU sensitivity and modeling using pico-second pulsed laser stimulation of a D Flip-Flop in 40 nm CMOS technology,” DFTS 2015.

# Agenda

I. Introduction

II. Theory of laser fault injection

Physics and basics of laser fault injection

Fault models of LFI

III. Static LFI experimental results

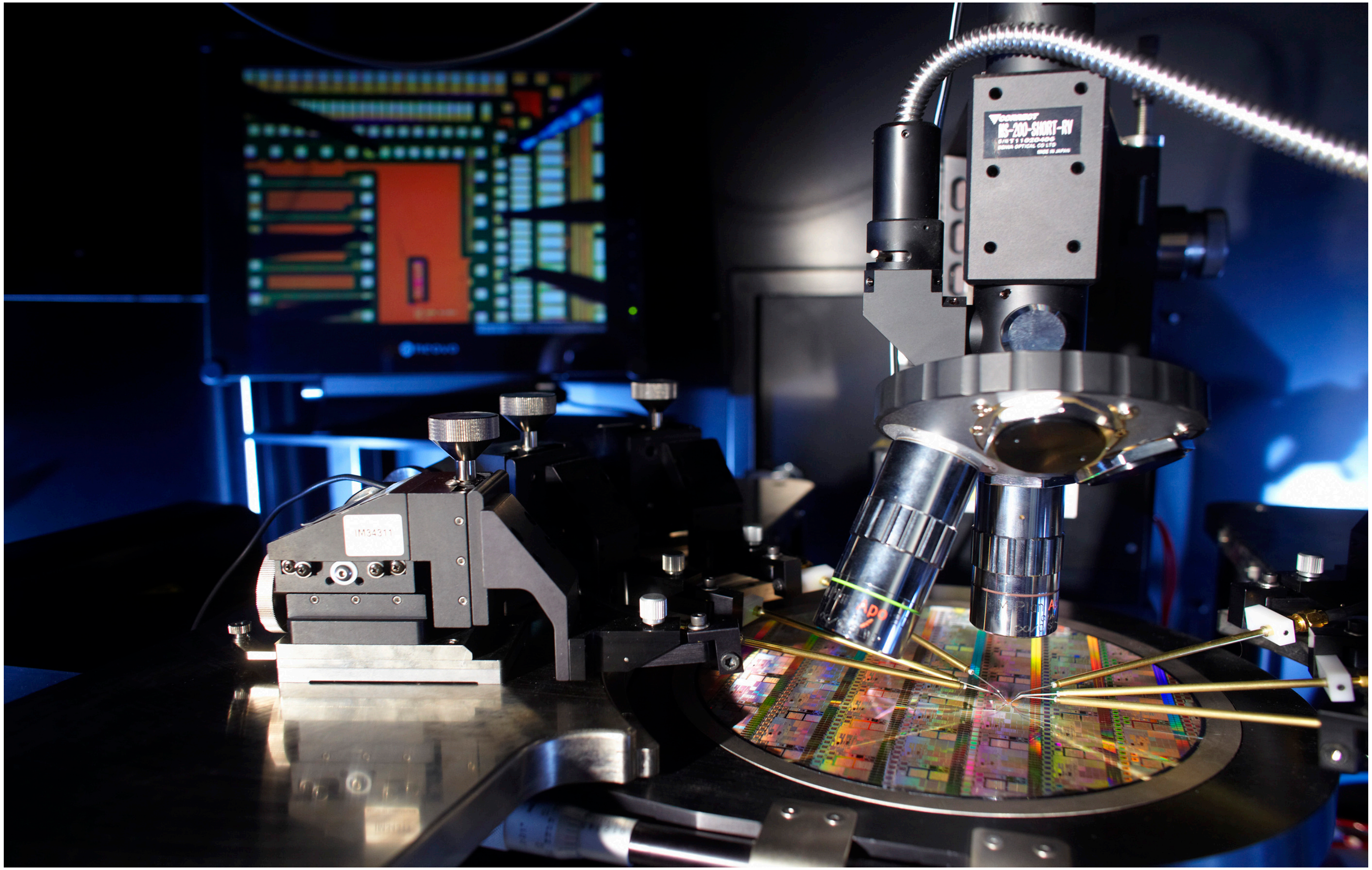
Setup, results, analysis

IV. Dynamic LFI experimental results

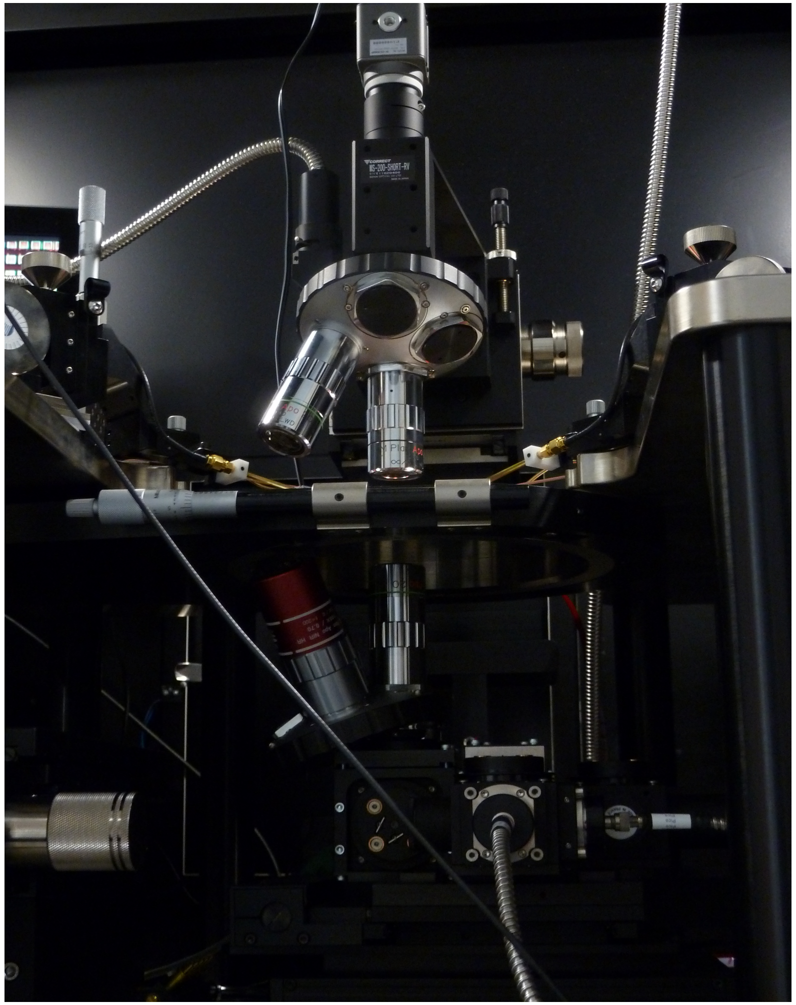
Setup, results, analysis

V. Conclusion

## ❑ Experimental setup

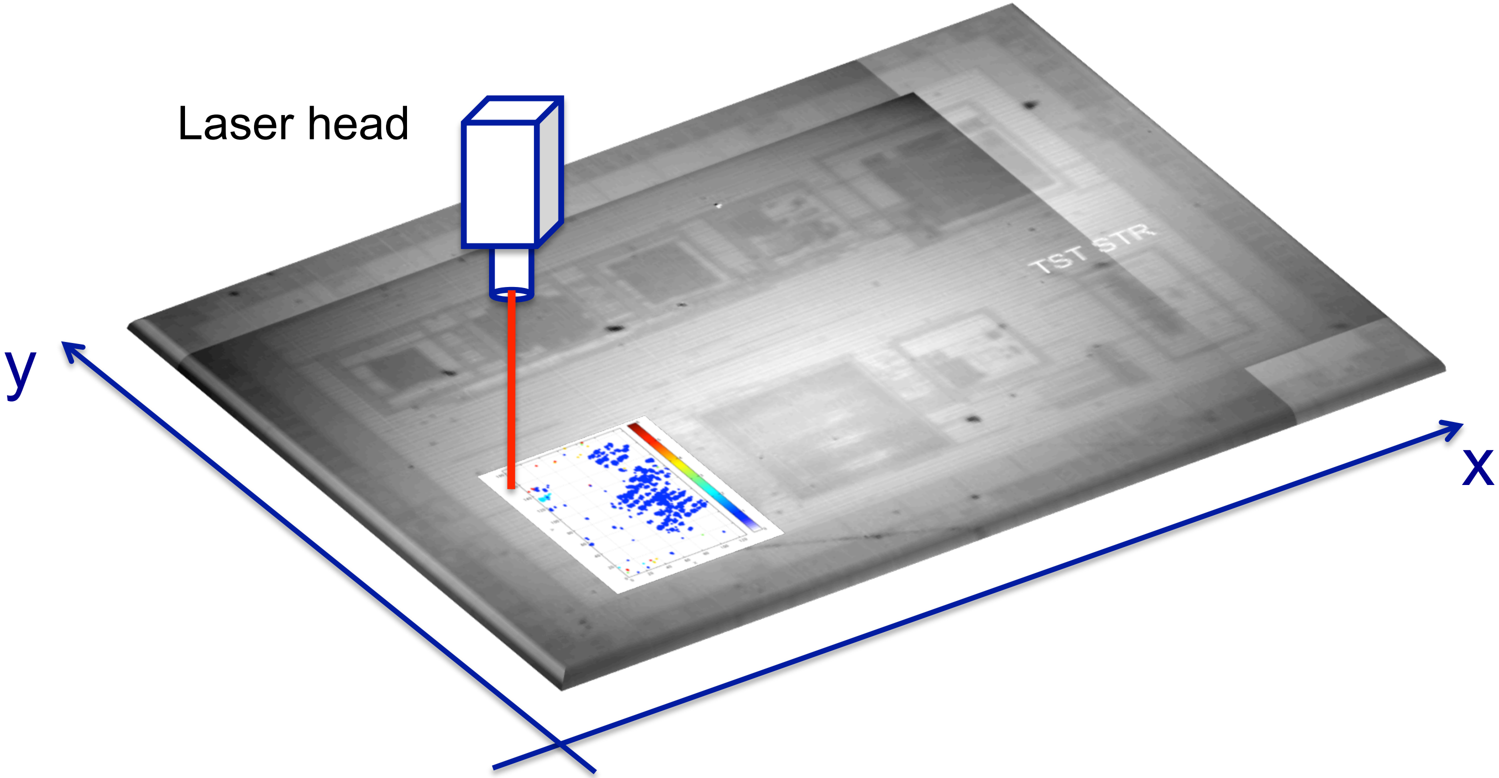


## ❑ Experimental setup



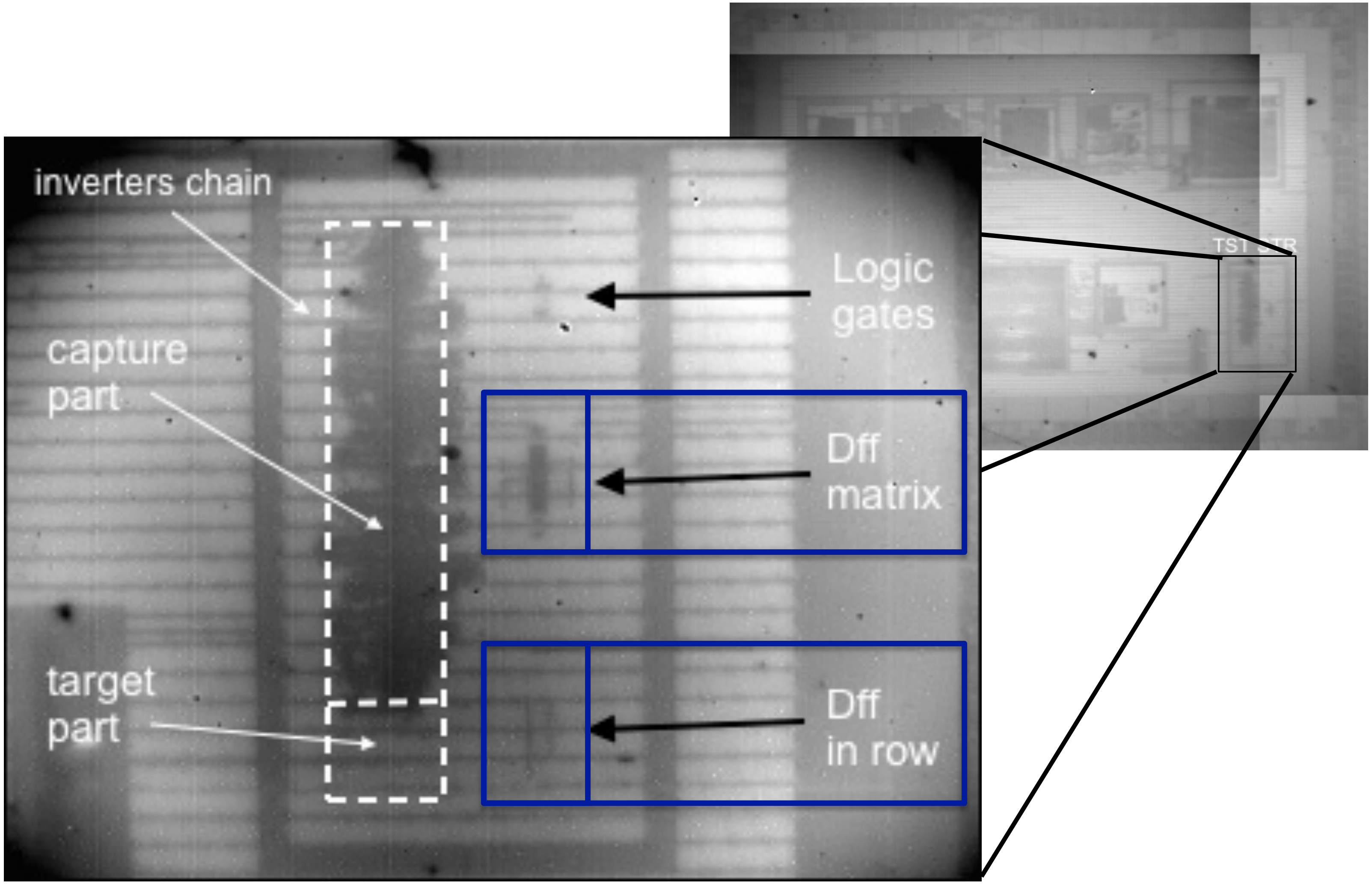
- Backside injection
- Pulse width: 30 ps
  - up to 100 nJ
- Wavelength: 1,030 nm
- Pulse width: ns
  - 5-50 ns, max. power 1 W
  - 50 ns – 1 s, max. power 3 W
- Wavelength: 1,064 nm
- Spot size: 1µm or 5 µm

## ❑ Experiments description



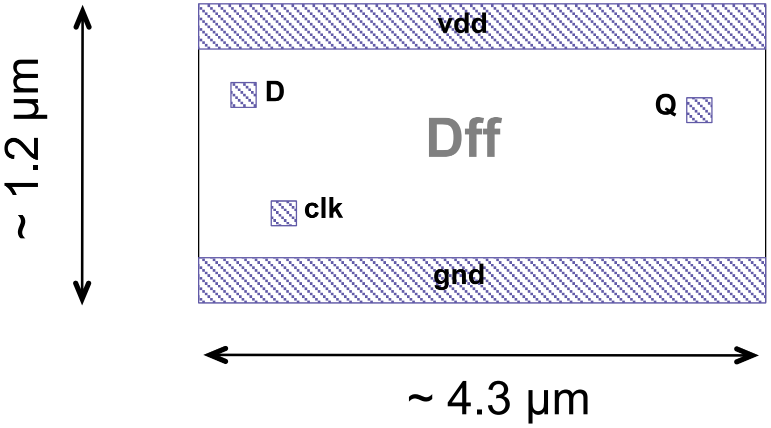
⇨ Laser fault sensitivity maps drawing
(colors according to the fault model)

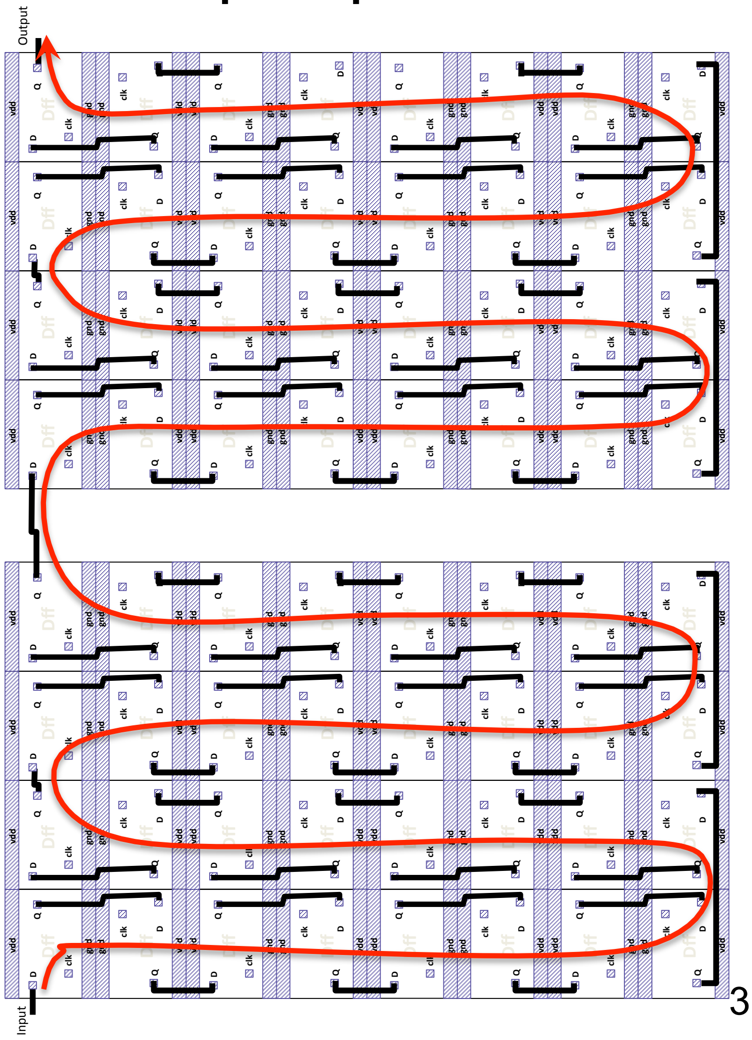
## ❑ Custom D flip-flop registers, CMOS 28 nm



## ❑ Custom D flip-flop registers, CMOS 28 nm

- Matrix shaped shift register with 64 D flip-flops



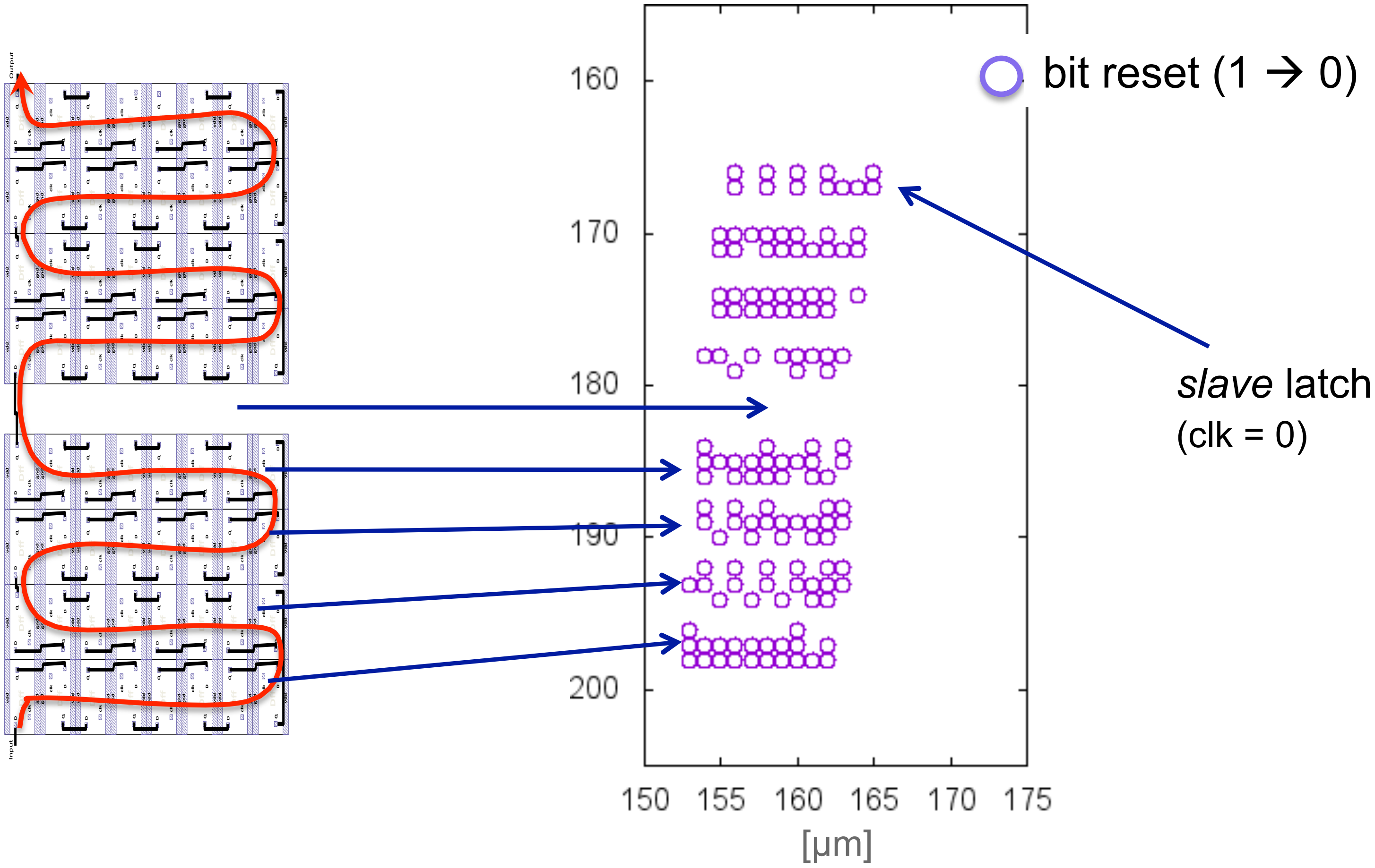


- DFF: ~ 40 transistors,

- *large* output buffer

## ❑ Custom D flip-flop registers, CMOS 28 nm

- spot 1 µm / **30 ps** / 0.5 nJ / Δxy = 1 µm / backside

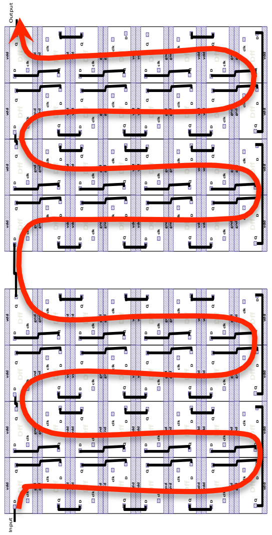


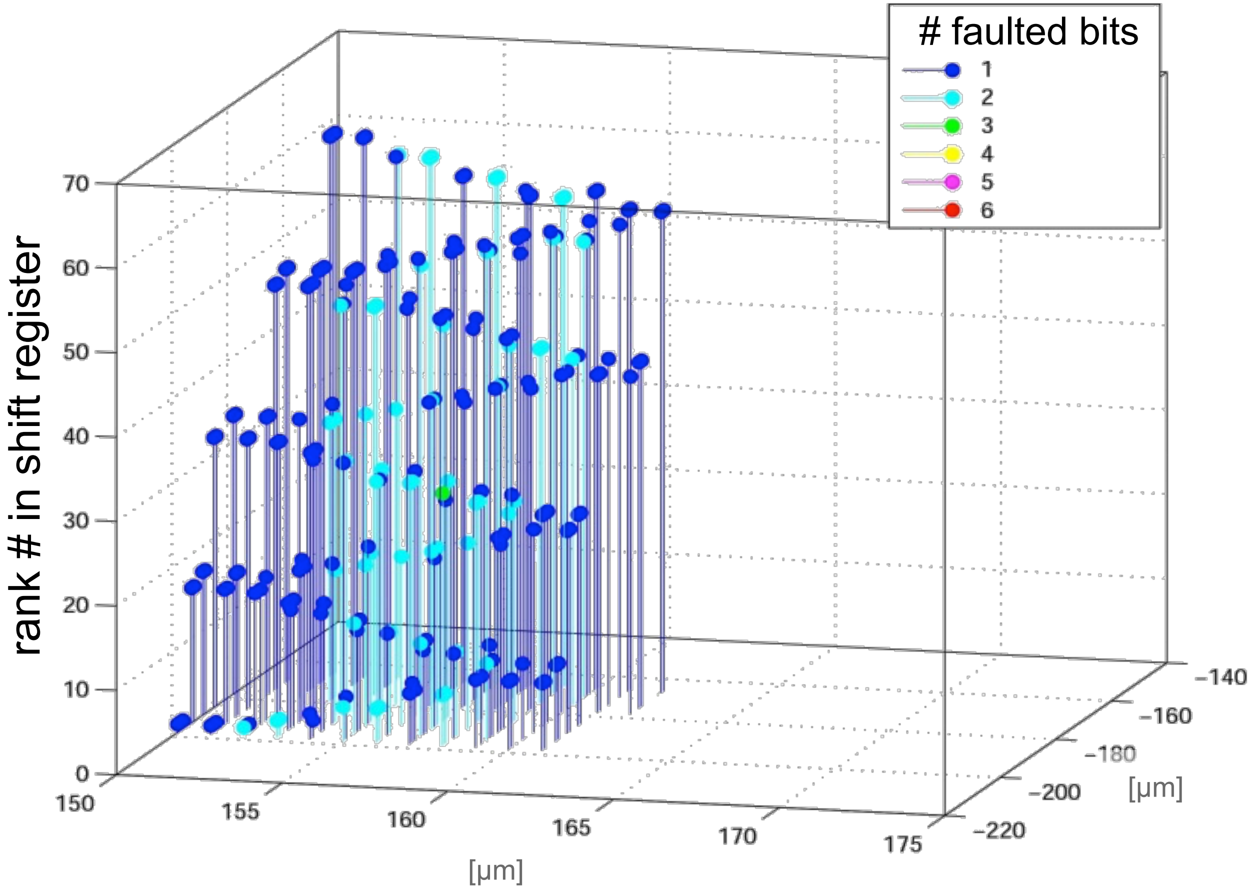
○ bit reset (1 → 0)

*slave* latch
(clk = 0)

## ❑ Custom D flip-flop registers, CMOS 28 nm

- 3D view at 1 nJ

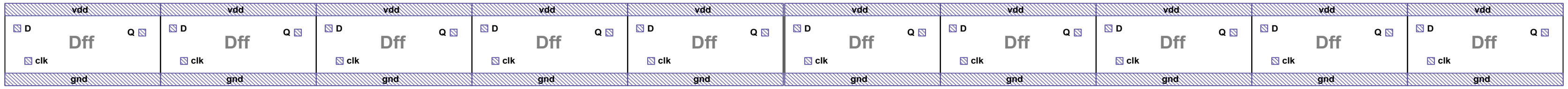




# III. Static LFI experimental results

## ❑ Custom D flip-flop registers, CMOS 28 nm

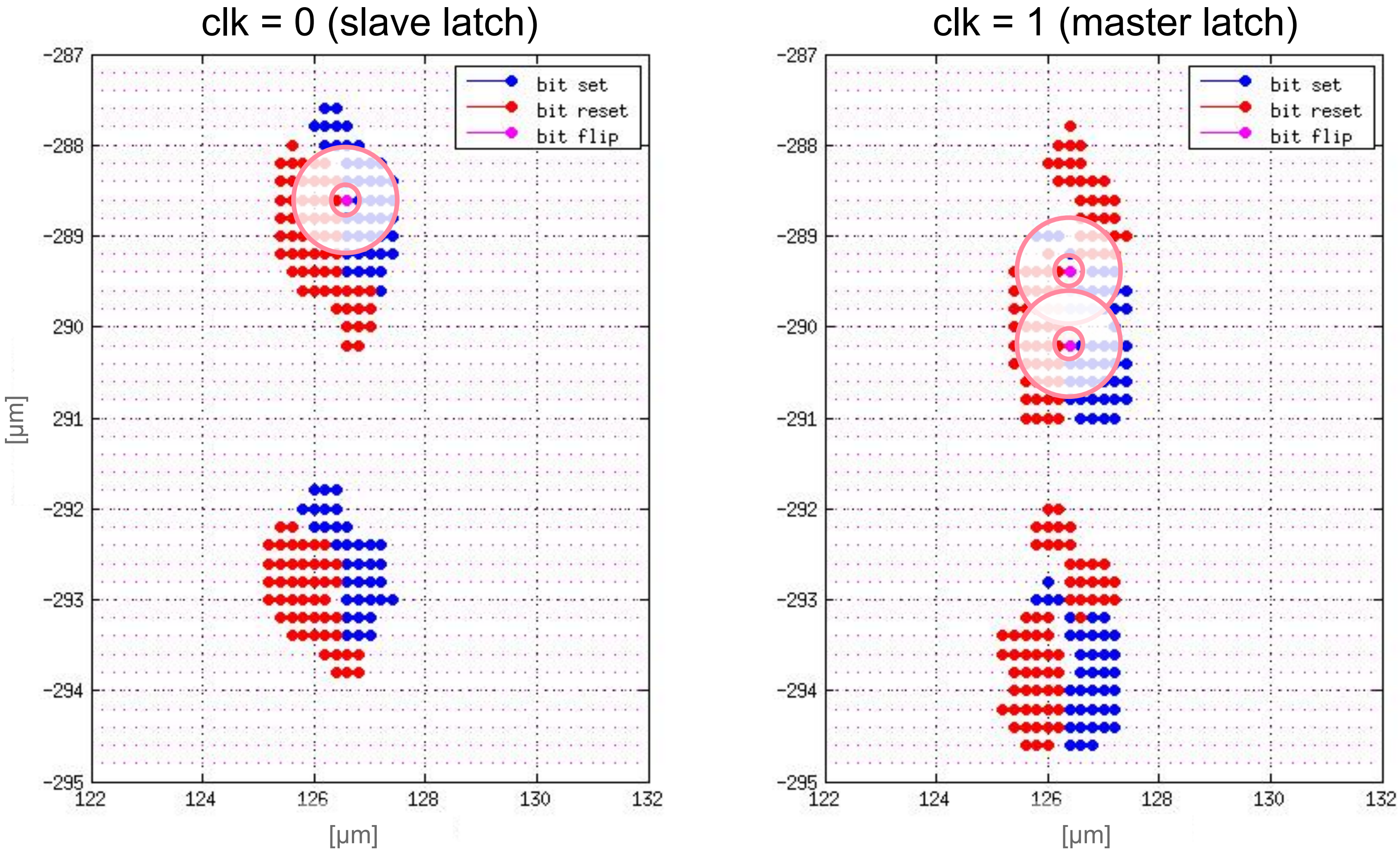
- in-line shift register with 10 D flip-flops



# III. Static LFI experimental results

## ❑ Custom D flip-flop registers, CMOS 28 nm

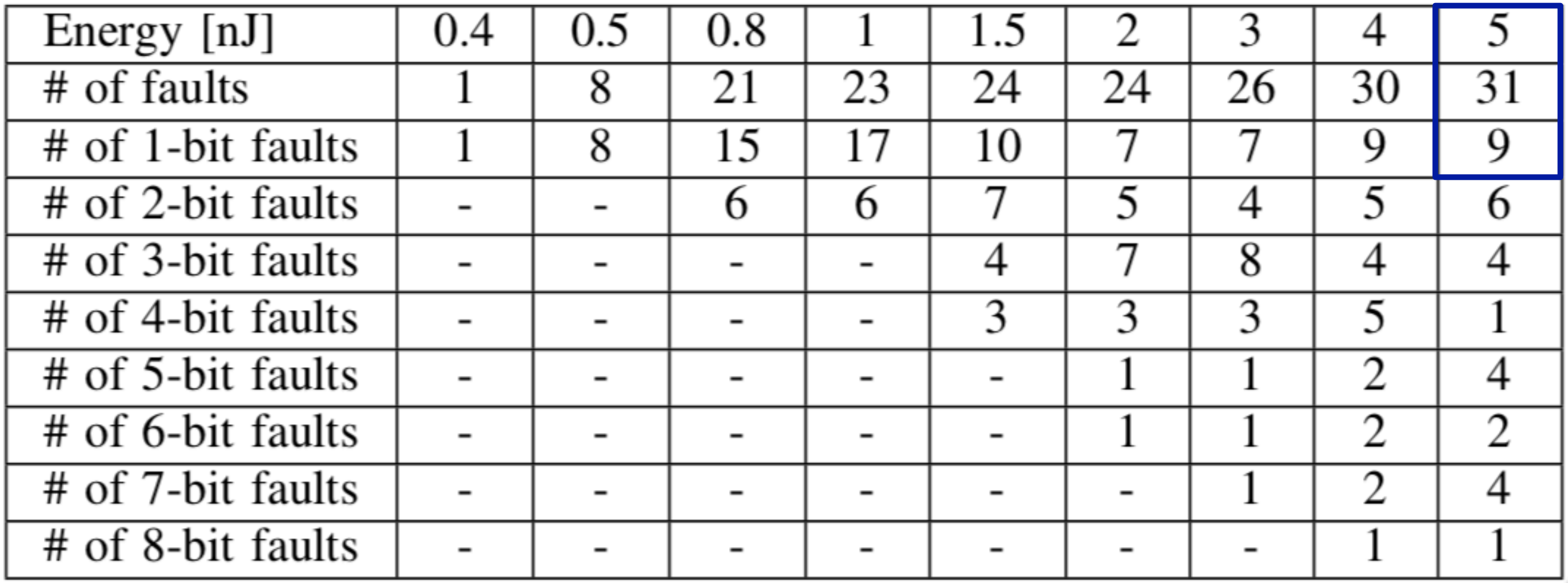
- spot 1 µm / **30 ps** / 0.5 nJ / Δxy = 0.2 µm / backside



## ❑ Memory elements, static test – Conclusion

Bit-set/reset fault model = relevant

Single-bit fault model experimentally assessed with a laser at the CMOS 28 nm node for 1 µm and 5 µm (see table below) laser spots.



| Energy [nJ] | 0.4 | 0.5 | 0.8 | 1 | 1.5 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|---|---|
| # of faults | 1 | 8 | 21 | 23 | 24 | 24 | 26 | 30 | 31 |
| # of 1-bit faults | 1 | 8 | 15 | 17 | 10 | 7 | 7 | 9 | 9 |
| # of 2-bit faults | - | - | 6 | 6 | 7 | 5 | 4 | 5 | 6 |
| # of 3-bit faults | - | - | - | - | 4 | 7 | 8 | 4 | 4 |
| # of 4-bit faults | - | - | - | - | 3 | 3 | 3 | 5 | 1 |
| # of 5-bit faults | - | - | - | - | - | 1 | 1 | 2 | 4 |
| # of 6-bit faults | - | - | - | - | - | 1 | 1 | 2 | 2 |
| # of 7-bit faults | - | - | - | - | - | - | 1 | 2 | 4 |
| # of 8-bit faults | - | - | - | - | - | - | - | 1 | 1 |

# Agenda

I. Introduction

II. Theory of laser fault injection

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

III. Static LFI experimental results

- Setup, results, analysis

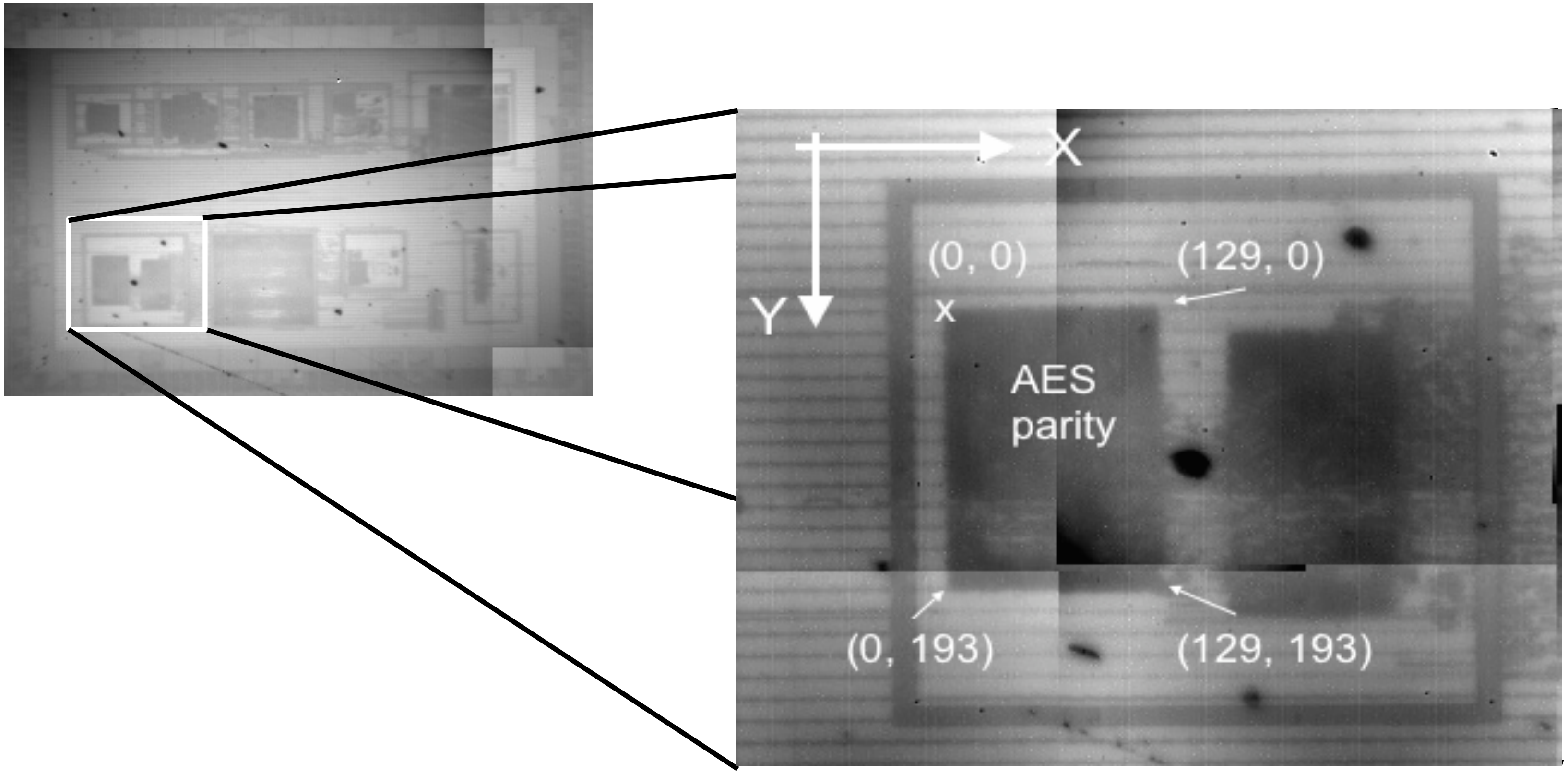
IV. Dynamic LFI experimental results

- Setup, results, analysis

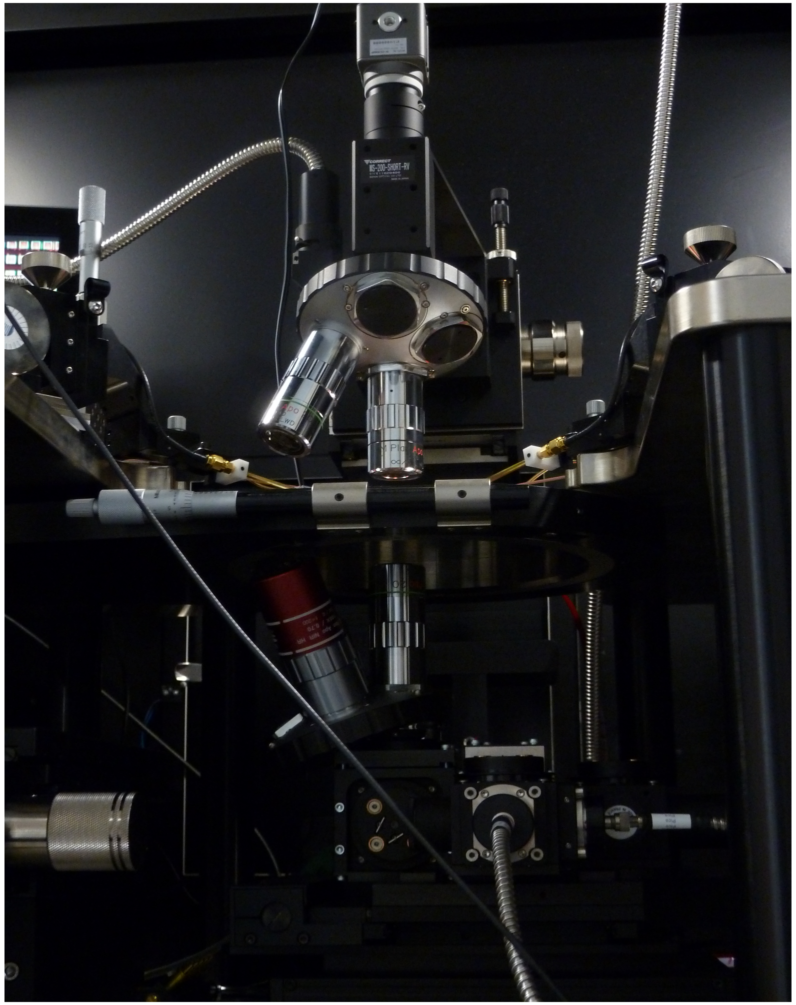
V. Conclusion

## ❑ Test chips CMOS 28 nm

- Target: AES implementation (with parity-based CM, 100 MHz)
  - IR microphotography (rear side), obj. x20



## ❑ Experimental setup

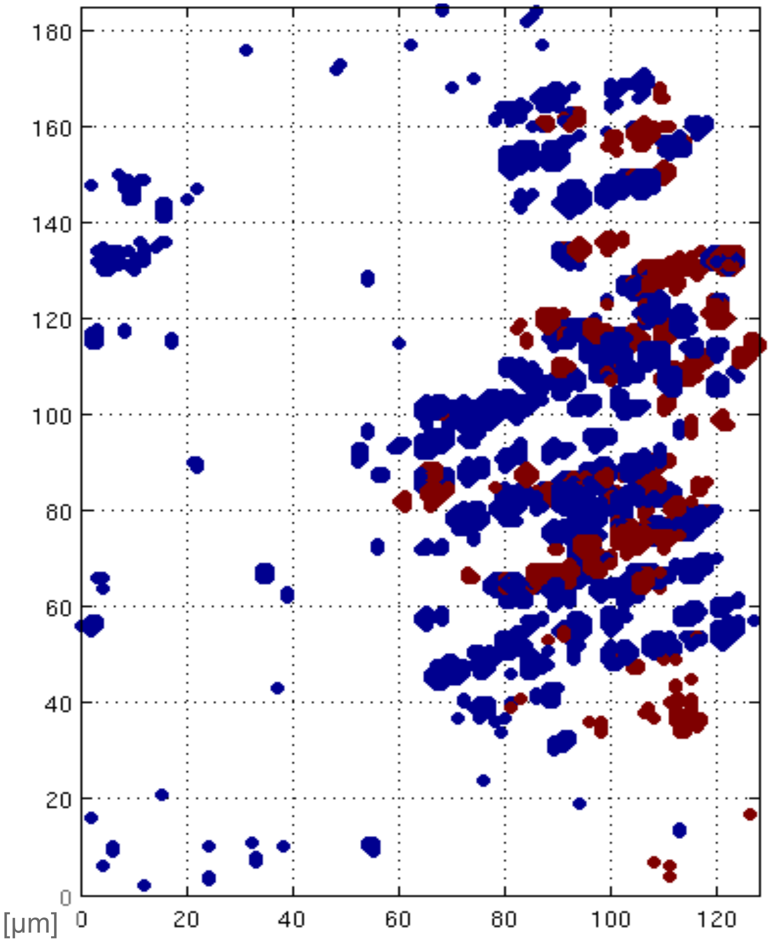


- Backside injection
- Pulse width:  30 ps
  - up to 100 nJ
- Wavelength: 1,030 nm
- Pulse width:  ns
  - 5-50 ns, max. power 1 W
  - 50 ns – 1 s, max. power 3 W
- Wavelength: 1,064 nm
- Spot size: 1µm or 5 µm

# IV. Dynamic LFI experimental results

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

  Exp.: 5 µm spot, 10 ns, 0.6-1.0 W, ∆xy = 1µm



26,380 faulted cipher texts

🔴 Unidentified faults: 6,574 (24.9 %)

mainly 5 – 8 faulty bytes (up to12)

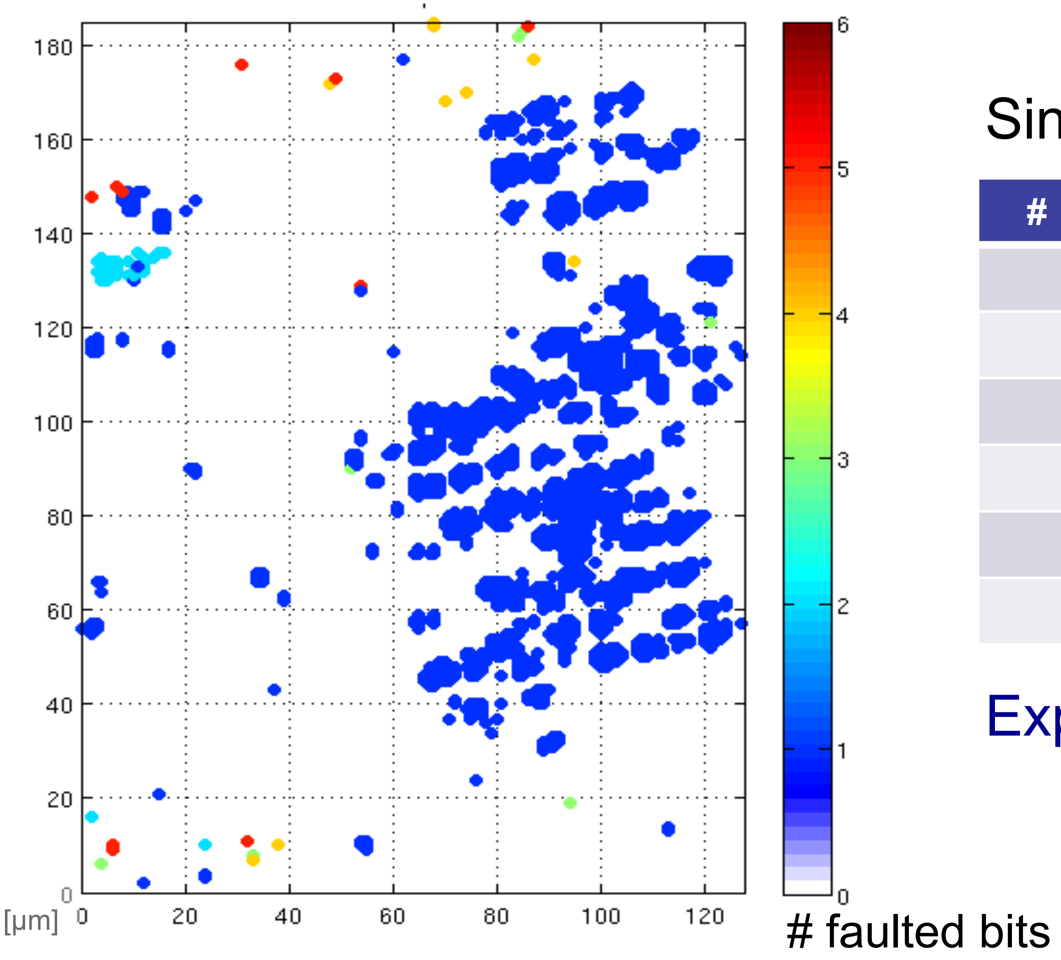
🔵 Identified faults: 19,806

single-byte faults

# IV. Dynamic LFI experimental results

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

  Exp.: 5 µm spot, 10 ns, 0.6-1.0 W, ∆xy = 1µm



## Single-byte faults analysis

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

Exp. single-bit LFI rate: 73.6 %

# Agenda

I. Introduction

II. Theory of laser fault injection

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

III. Static LFI experimental results

- Setup, results, analysis

IV. Dynamic LFI experimental results

- Setup, results, analysis

V. Conclusion

# Conclusion

□ Exp. LFI fault model analysis at CMOS 28 nm

□ Single-bit: static & dynamic tests (~ 70% success rate)
1 µm & 5 µm laser spot size
ps & ns laser pulse duration

□ Data dependence: bit-set/reset on D flip-flops
well defined sensitive areas

Single-bit & Bit-set/reset are still actual and practical fault models at advanced CMOS technology nodes (28 nm).

Q? Does it still holds at the CMOS 14 nm node?

Thank you for your attention

dutertre@emse.fr

Work funded by the ANR: LIESSE project
ANR-12-INS-0008-01

PROJET FINANCÉ PAR L'ANR
ANR
PROJECT FUNDED BY THE ANR

J.M. Dutertre[1], V. Beroulle[2], P. Candelier[3], S. De Castro[1,4], L.B. Faber[3], M.L. Flottes[4], P. Gendrier[3], D. Hély[2], R. Leveugle[5], P. Maistri[5], G. Di Natale[4], A. Papadimitriou[2], B. Rouzeyre[4]

(1) MINES Saint-Étienne
Une école de l'IMT
Institut Mines-Télécom

(2) LCIS

(3) life.augmented

(4) LIRMM

(5) tima
CNRS - Grenoble INP - UGA