EUROPEAN COOPERATION IN SCIENCE AND TECHNOLOGY

TRUDEVICE - WG Meetings

Trustworthy Manufacturing and Utilization of Secure Devices

Laser-Induced Faults in SRAM Memory Cells:

Experimental Results and Simulation-based Analysis

J.-M. Dutertre[1], C. Roscian[1], A. Sarafianos[2], M. Lacruche[1]

December 13th 2013 – Freiburg – Germany

1: Département SAS - Centre Microélectronique de Provence - 880, route de Mimet, 13541 Gardanne

2: STMicroelectronics, Avenue Célestin Coq 13790 Rousset, France

Ecole Nationale Supérieure des Mines SAINT-ETIENNE Site Georges Charpak

life.augmented

I. Introduction

Laser fault injection – mechanism

SRAM fault injection sensitivity

II. Fault model

Description & Assumptions

III. Experimental results

Standalone SRAM / μCTRL RAM

IV. Model-based simulation of laser-induced faults

V. Conclusion and perspectives

❑ Laser-induced fault injection – mechanism

- The inverter case

Sensitive area: reverse biased PN junction (drain of the off transistor)

laser => photocurrent => voltage transient (SET)

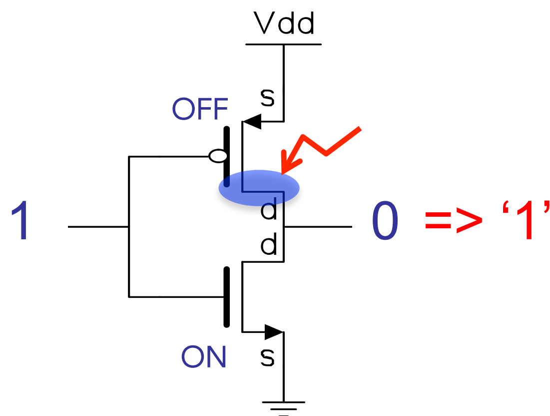
sensitive area (data dependent)

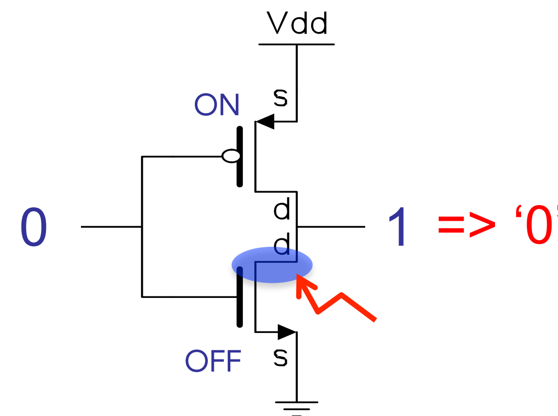
❑ Laser-induced fault injection – mechanism

- The inverter case

Sensitive area: reverse biased PN junction (drain of the off transistor)

laser => photocurrent => voltage transient (SET)



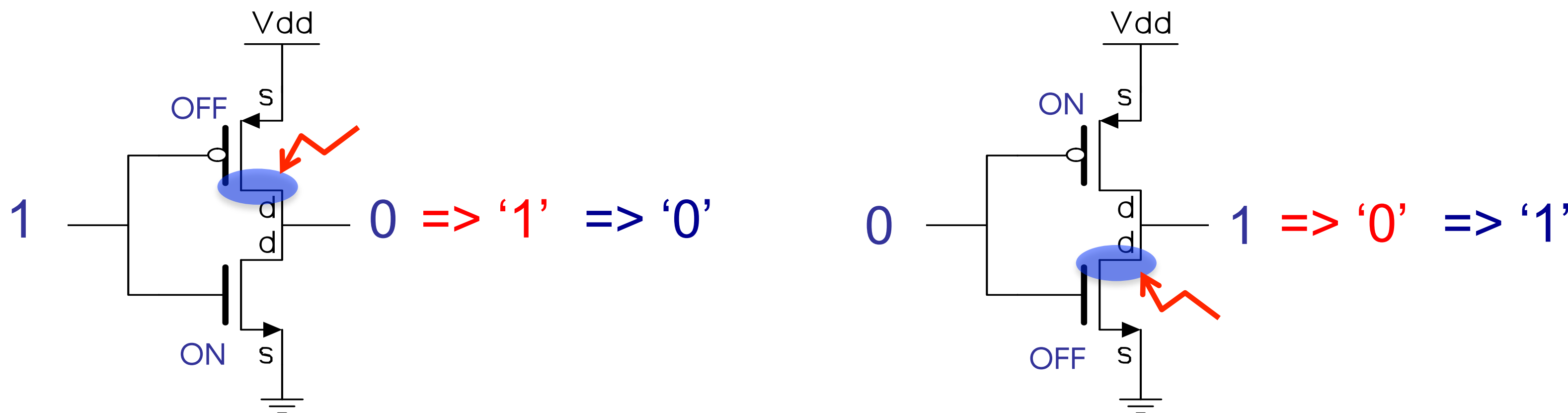


❑ Laser-induced fault injection – mechanism

- The inverter case

Sensitive area: reverse biased PN junction (drain of the off transistor)

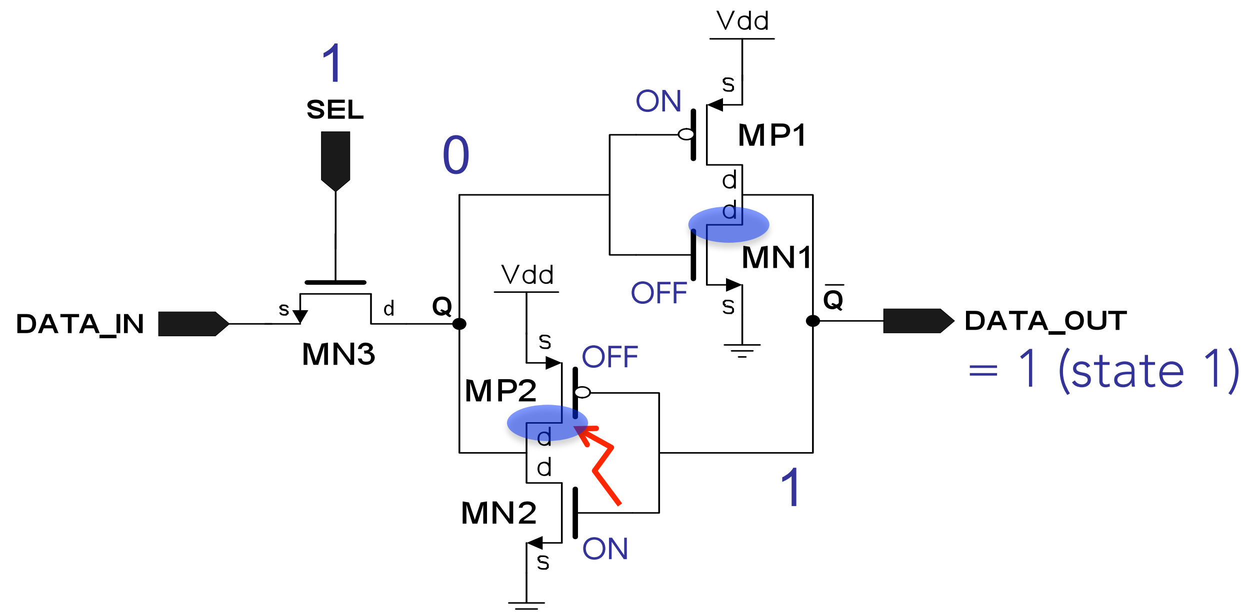
laser => photocurrent => voltage transient (SET)



sensitive area (data dependent)

❑ Laser-induced fault injection – mechanism (cont.)

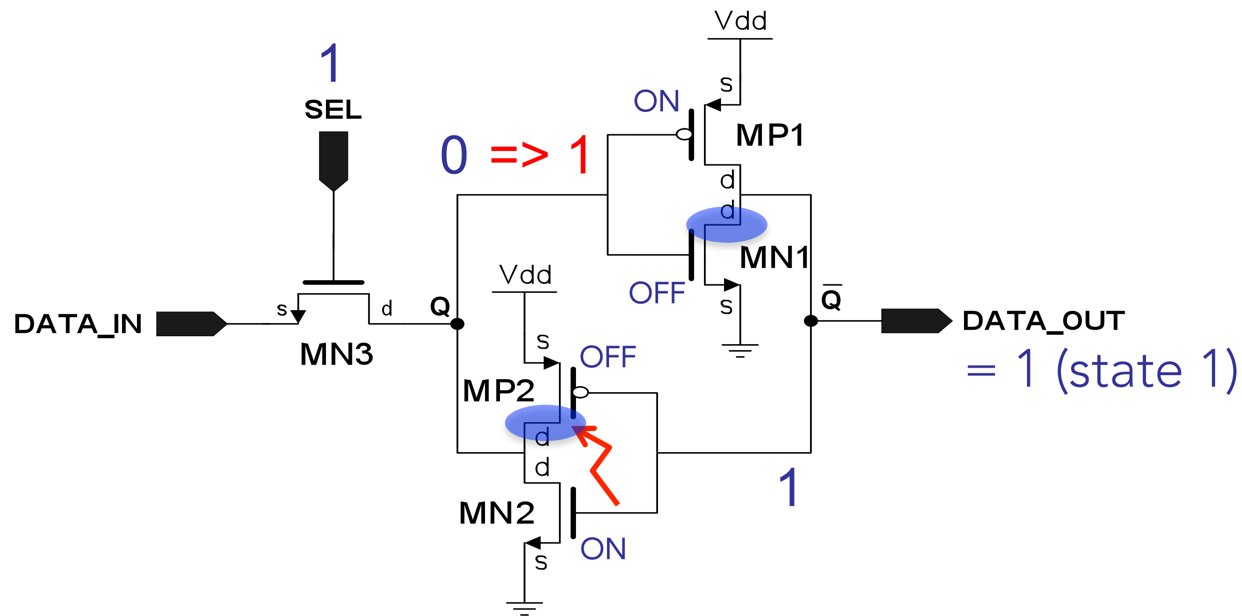
- Single Event Upset in a SRAM cell (5T CSRAM)



sensitive area (data dependent)

❑ Laser-induced fault injection – mechanism (cont.)

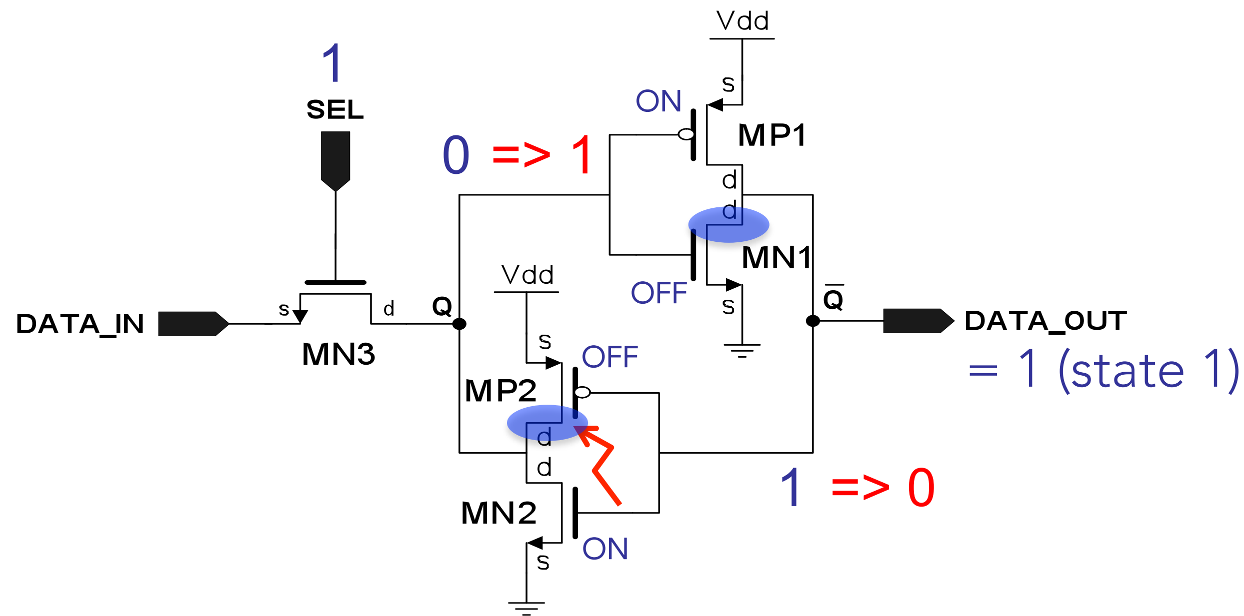
- Single Event Upset in a SRAM cell (5T CSRAM)



sensitive area (data dependent)

❑ Laser-induced fault injection – mechanism (cont.)

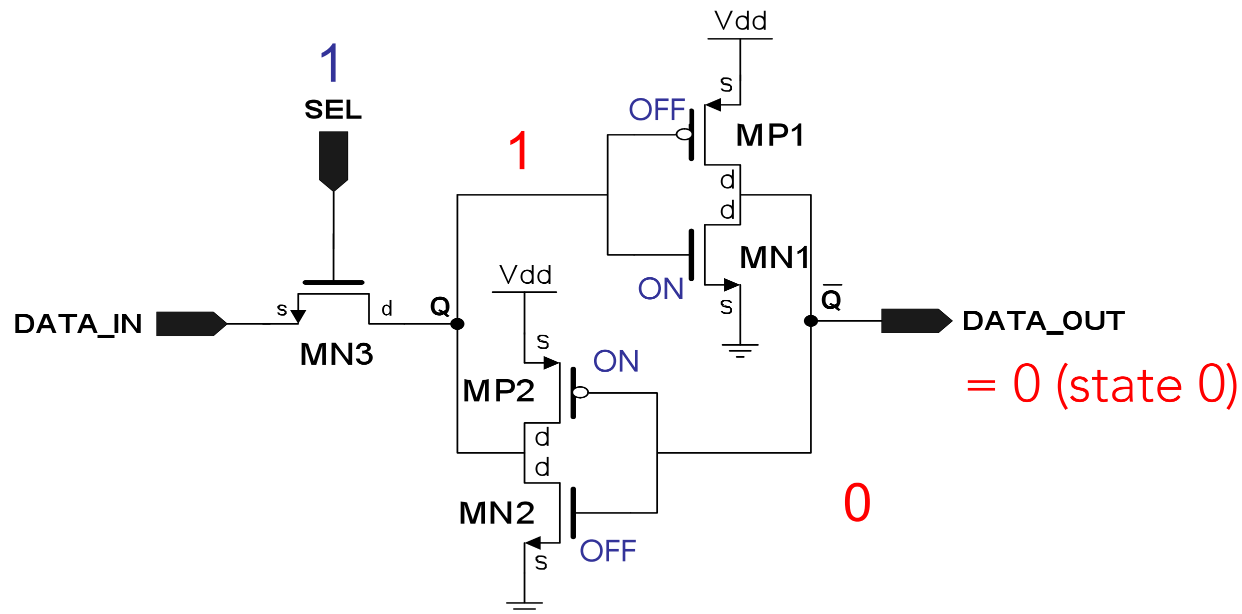
- Single Event Upset in a SRAM cell (5T CSRAM)



sensitive area (data dependent)

❑ Laser-induced fault injection – mechanism (cont.)

- Single Event Upset in a SRAM cell (5T CSRAM)



sensitive area (data dependent)

Fault model

- Bit-flip

$$\forall b \xrightarrow{\lightning} b' = \overline{b}$$

Usually assumed

- Bit-set / Bit-reset

Bit-set:
$$\text{if } b = 0 \xrightarrow{\lightning} b' = 1$$
$$\text{if } b = 1 \xrightarrow{\lightning} b' = 1$$

Bit-reset:
$$\text{if } b = 0 \xrightarrow{\lightning} b' = 0$$
$$\text{if } b = 1 \xrightarrow{\lightning} b' = 0$$

} data dependent

$\Rightarrow$ Permits Safe error attacks (e.g. on the key registers)

$\Rightarrow$ Provides additional information on the handled data

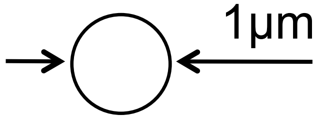
❑ SRAM fault model

CMOS 0.25µm – layout analysis

SEU sensitive areas:

- data dependent

Laser spot size:



⇒ Consistent with bit-set/reset

bit-set areas

bit-reset areas

4µm

9µm

Vdd

MP1

MP2

Q

data_out

SEL

MN2

MN1

MN3

Gnd

Metal 1

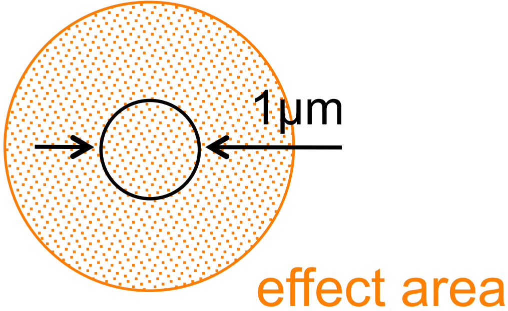
MOS gate

Diffusion

❑ SRAM fault model

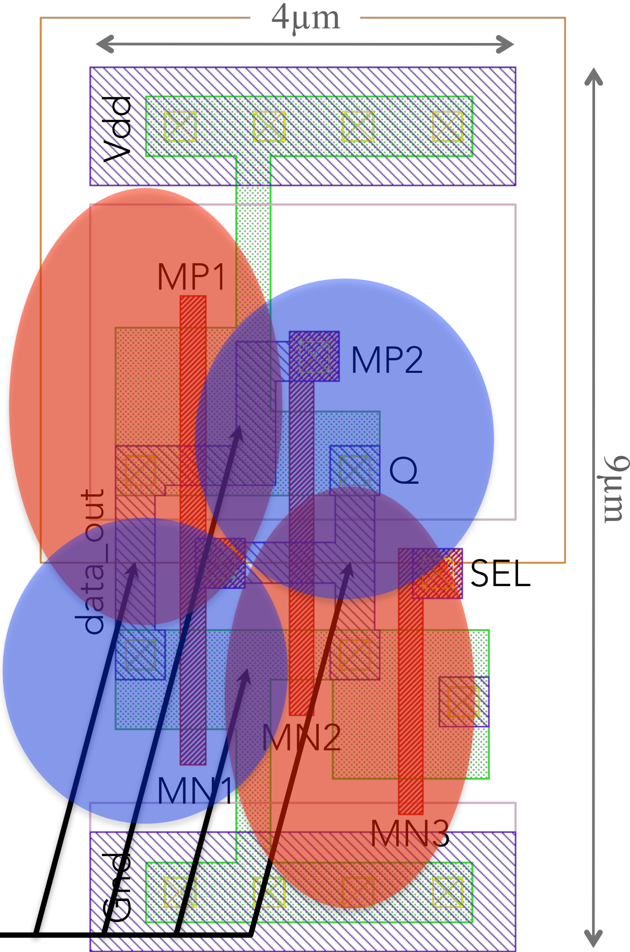
CMOS 0.25μm – layout analysis

Laser spot size:



⇒ Consistent with bit-flip

bit-flip areas

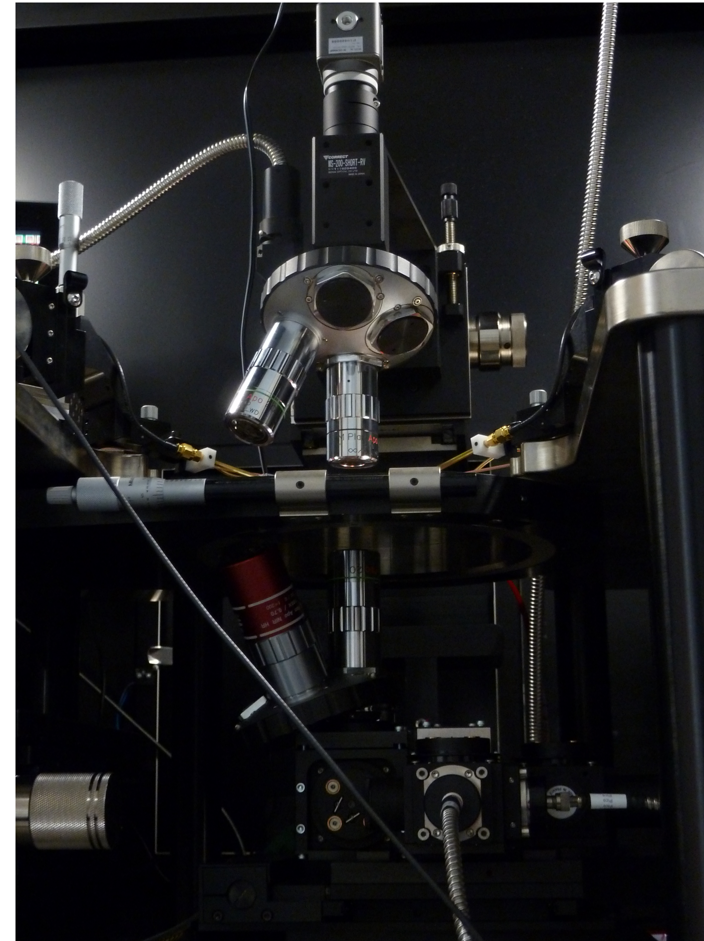


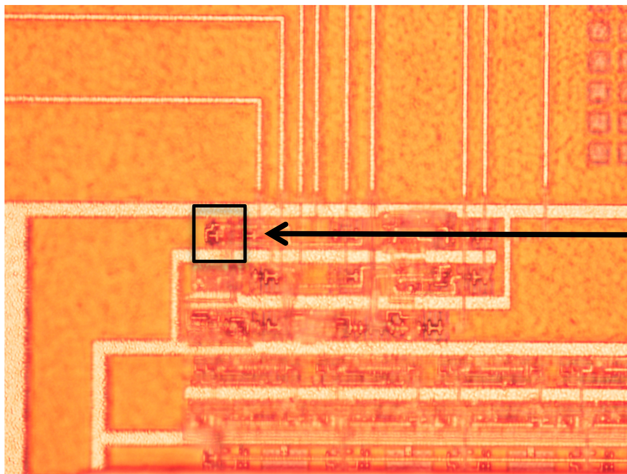
⇒ Combination of the two fault models?

state 1
state 0

❑ Experimental setup

- Frontside injection
- Wavelength: 1064nm (IR)
- Spot size: 1µm, 5µm
- Pulse width: 50ns, 30ps
- Power: 0.26W, 0.42W
- Scan steps: 0.2µm



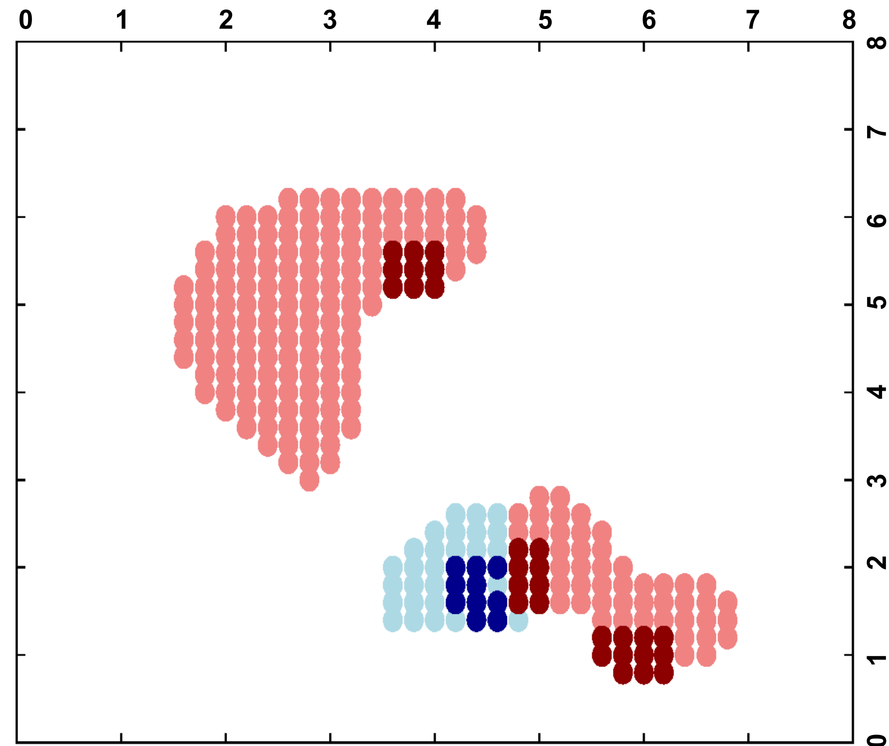


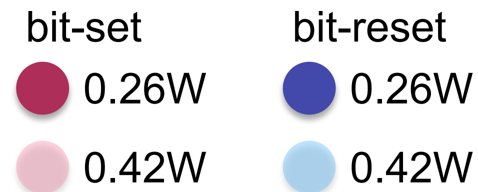
- SRAM 5T
- CMOS 0.25µm (test chip)

❑ Fault injection sensitivity map SRAM 5T 0.25μm ∅1μm

▪ no overlap between bit-set and bit-reset areas

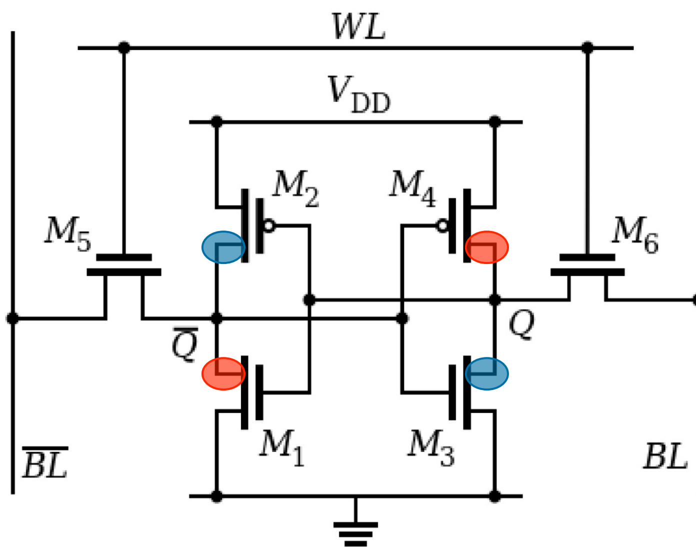
⇒ no bit-flips!

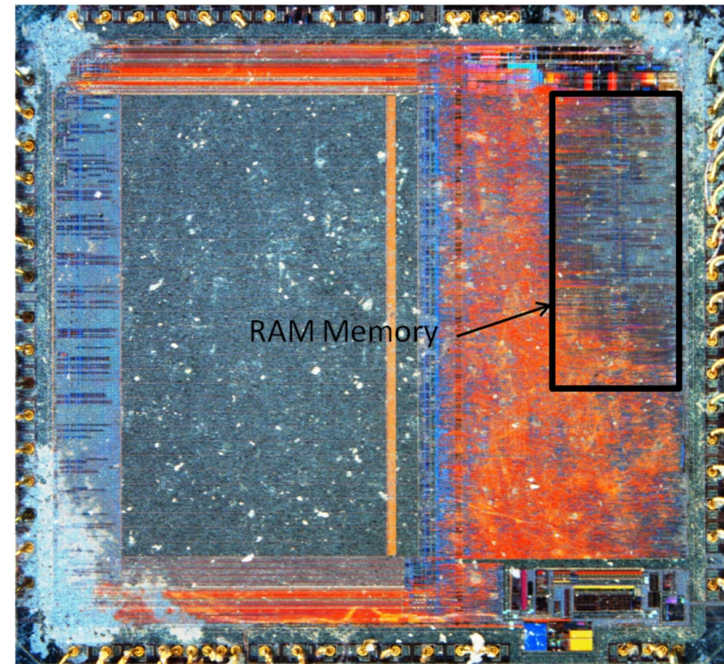




❑ Fault injection sensitivity map µCTRL RAM

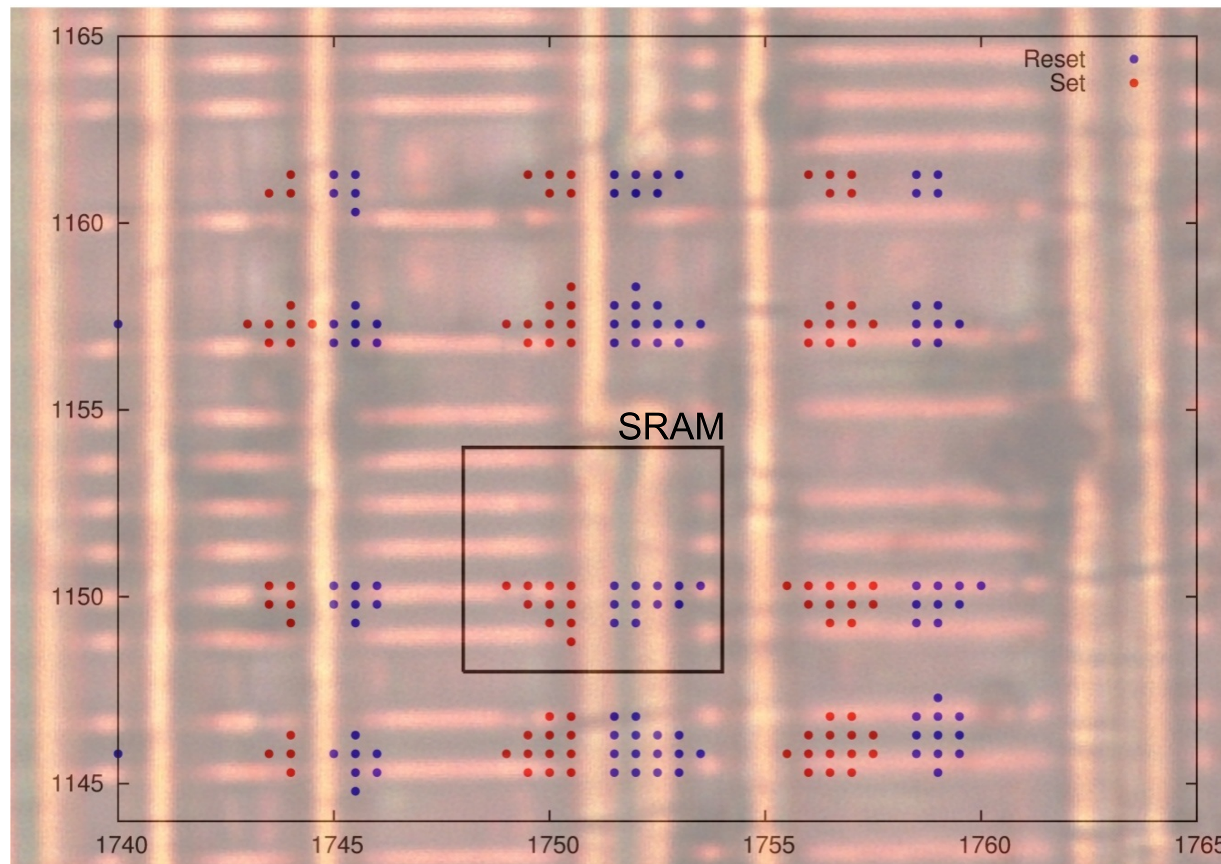
- 8-bit µCTRL
- CMOS 0.35µm
- target: RAM memory
- 6T SRAM cells





❑ Fault injection sensitivity map µCTRL RAM

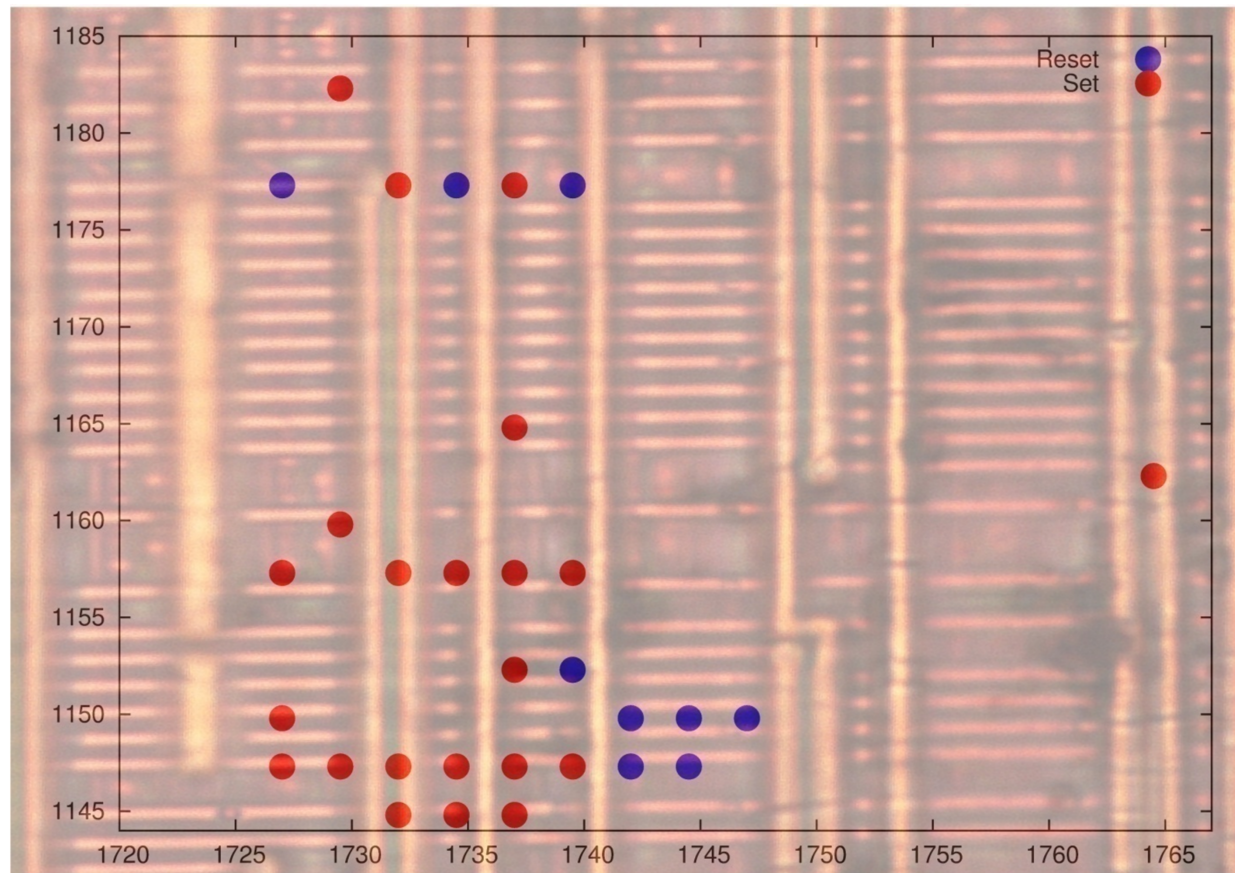
- Laser: ∅ 1µm / 0.29W / 50ns



⇒ fault model: bit-set/reset (no overlap)

❑ Fault injection sensitivity map µCTRL RAM

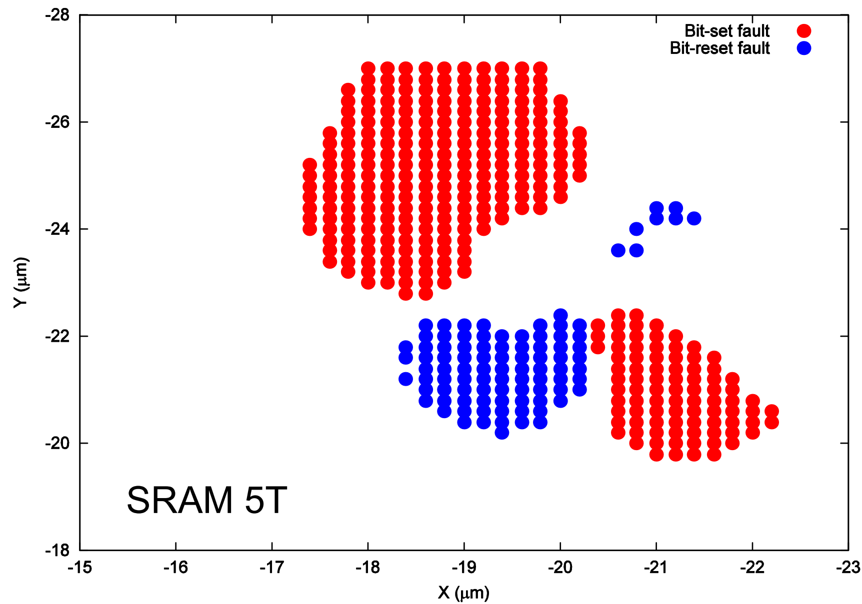
- Laser: ∅ 5µm / 0.29W / 50ns

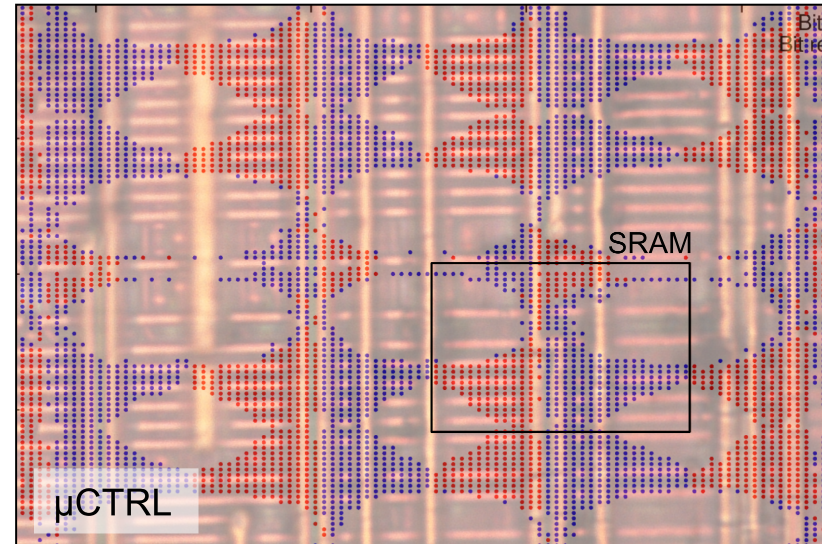


⇒ fault model: bit-set/reset (no overlap)

❑ Fault sensitivity map (cont.)

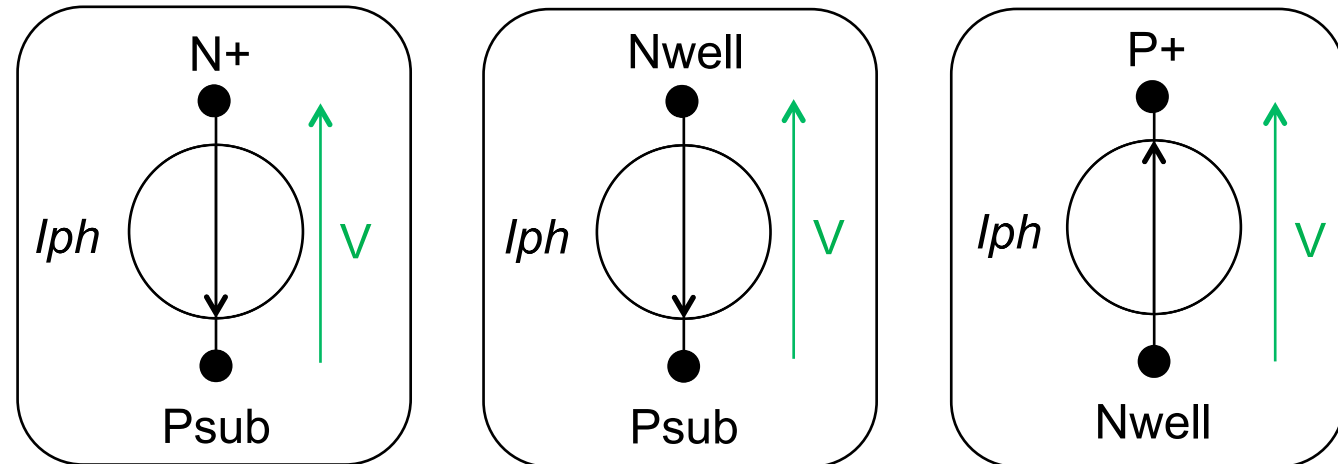
- Picoseconds range laser source
  - pulse duration: 30ps
  - energy: 26nJ





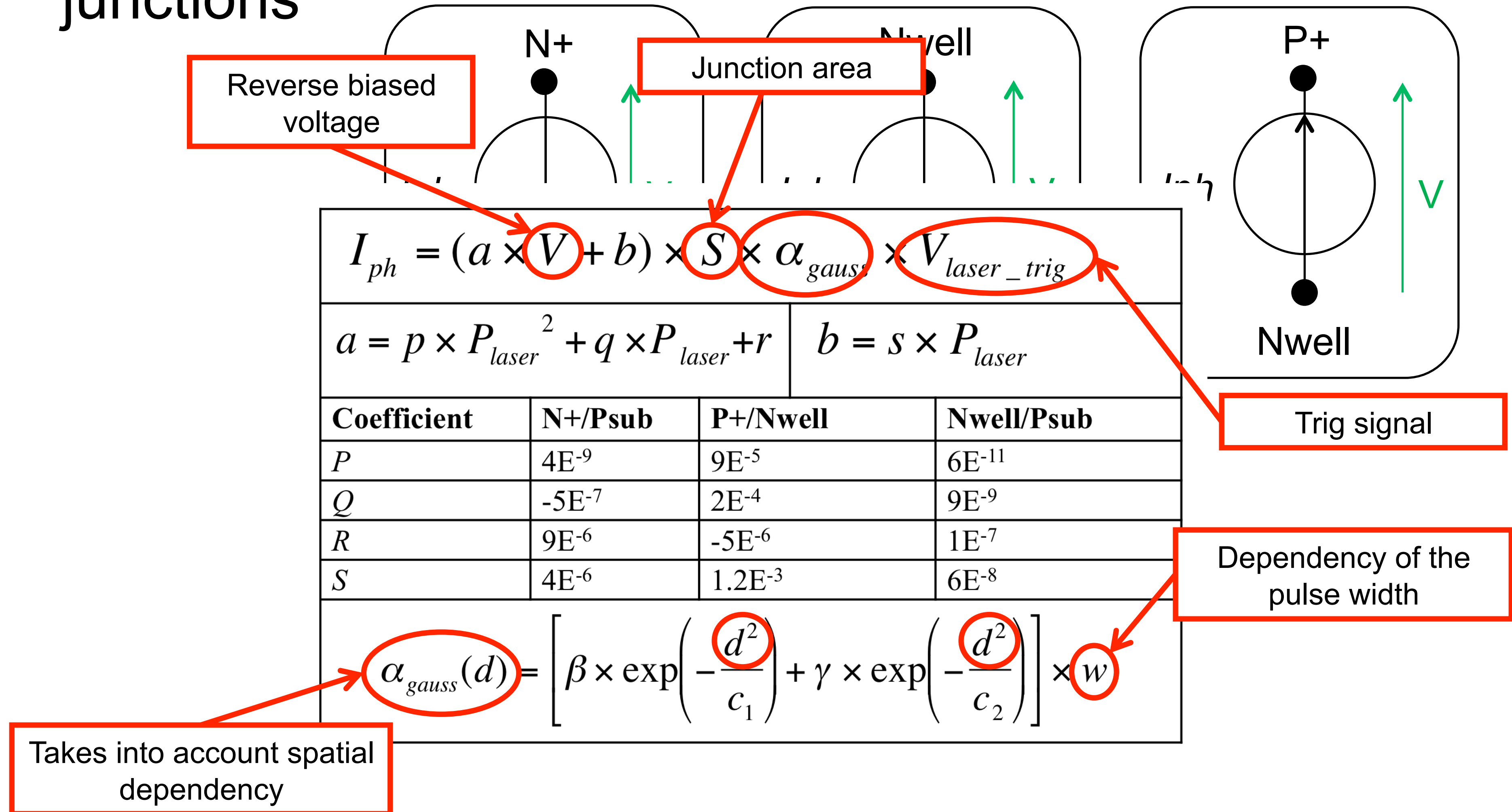
⇒ fault model: bit-set/reset

❑ Electrical modeling of photocurrents induced in PN junctions



Sarafianos et al., *Electrical modeling of the photoelectric effect induced by a pulsed laser applied to an SRAM cell*, Microelectronic Reliability

❑ Electrical modeling of photocurrents induced in PN junctions



$$I_{ph} = (a \times V + b) \times S \times \alpha_{gauss} \times V_{laser_trig}$$

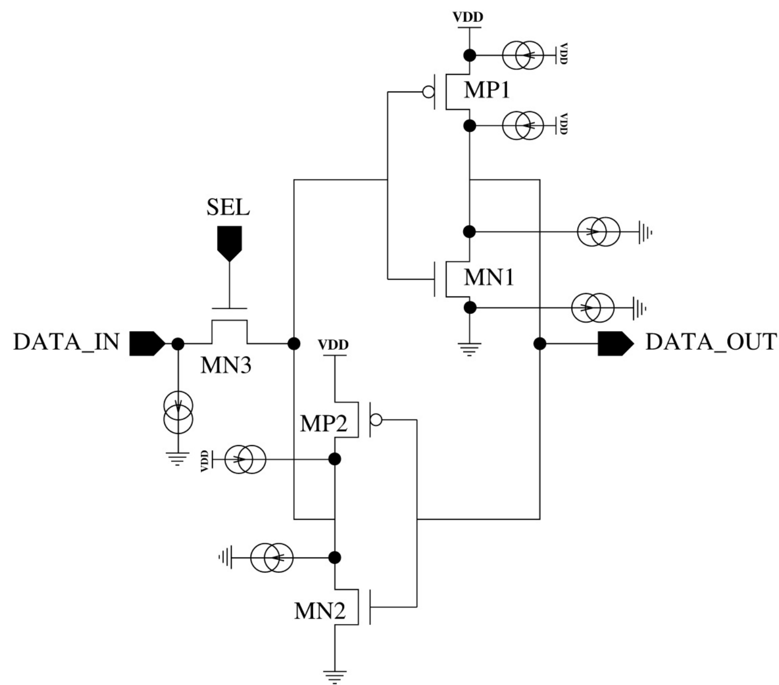
$$a = p \times P_{laser}^{2} + q \times P_{laser} + r \qquad b = s \times P_{laser}$$

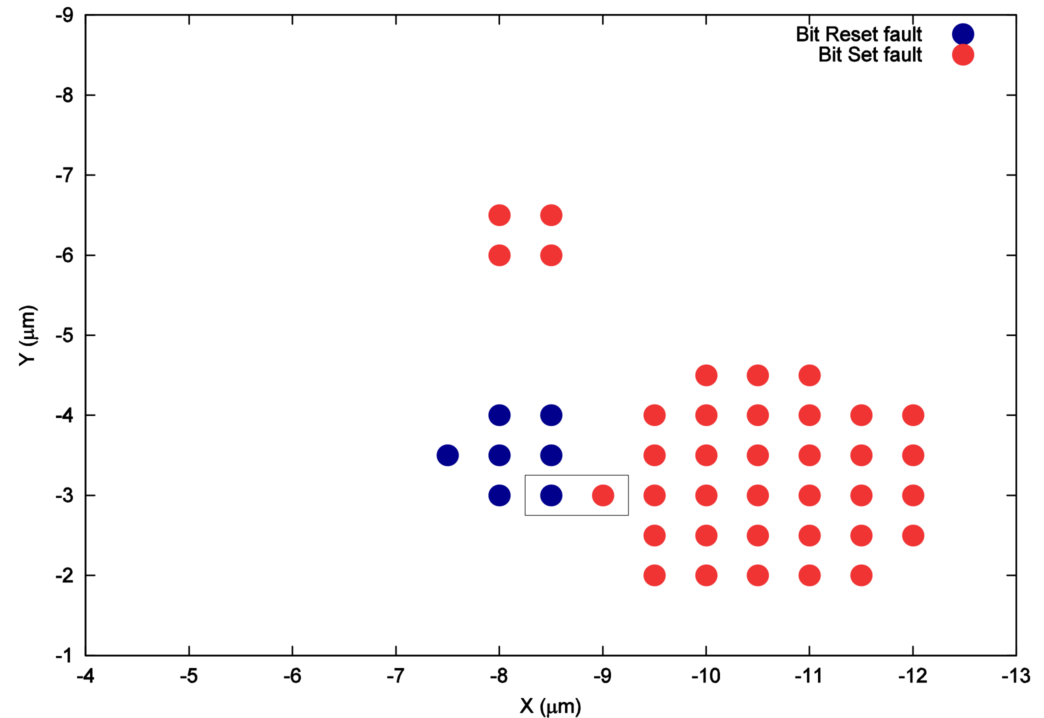
Coefficient	N+/Psub	P+/Nwell	Nwell/Psub
P	4E-9	9E-5	6E-11
Q	-5E-7	2E-4	9E-9
R	9E-6	-5E-6	1E-7
S	4E-6	1.2E-3	6E-8

$$\alpha_{gauss}(d) = \left[\beta \times \exp\left(-\frac{d^2}{c_1}\right) + \gamma \times \exp\left(-\frac{d^2}{c_2}\right)\right] \times w$$

Sarafianos et al., *Electrical modeling of the photoelectric effect induced by a pulsed laser applied to an SRAM cell*, Microelectronic Reliability

❑ Simulation-based SEU sensitivity map of an SRAM



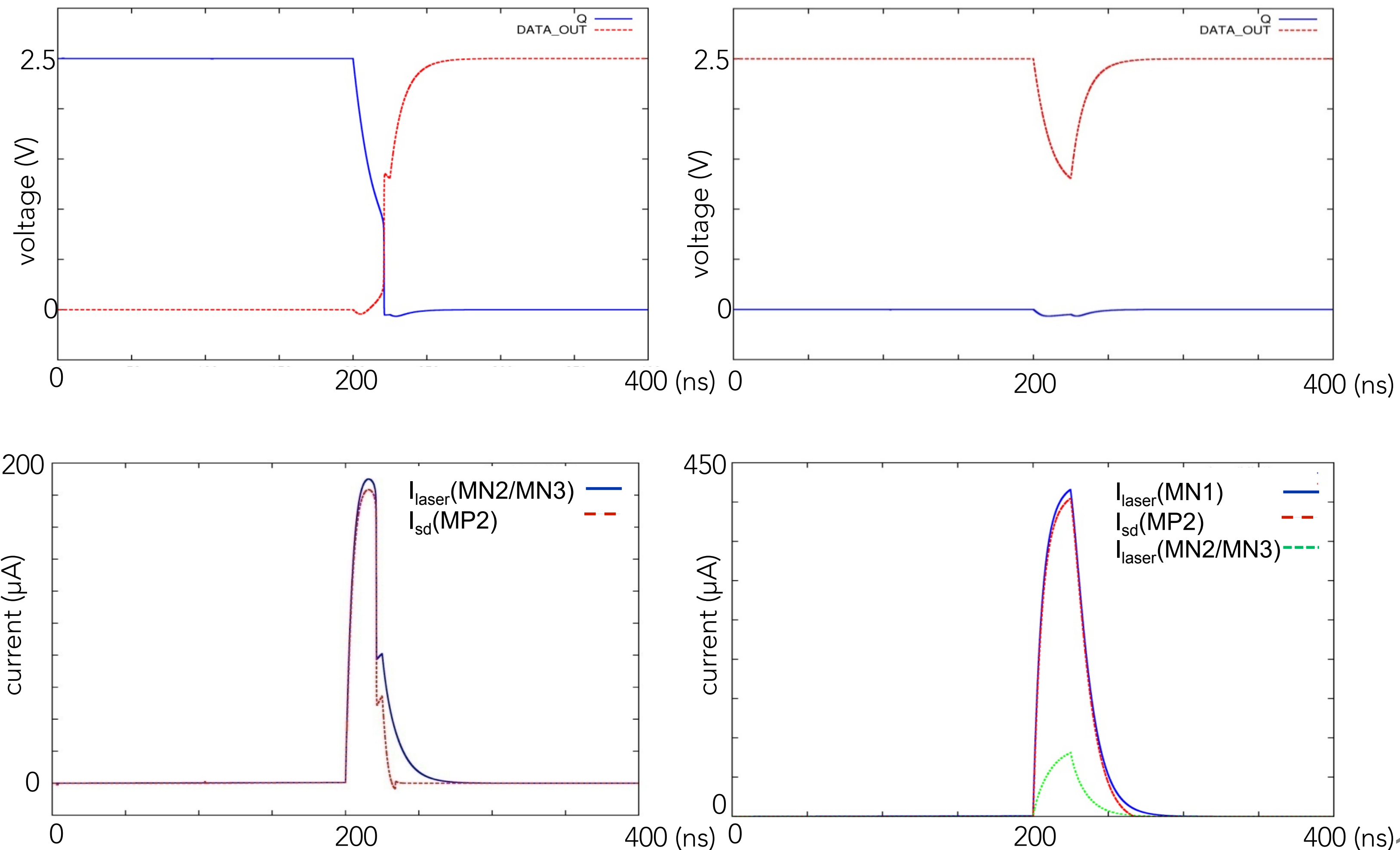


⇒ bit-set/reset fault model confirmed

⇒ qualitative results (model developed for 90nm)

❑ Simulation-based SEU sensitivity map of an SRAM

- Voltages and currents analysis explain the absence of bit-flips



❑ SRAM fault model laser injection

The relevant fault model is bit-set/reset ∅1-5µm / 30ps-50ns

On exp. and simulation basis

Only a few bit-flips (<1%) on µCTRL

❑ Perspectives

- More exp. tests (technologies, laser parameters)
- Extend laser effect modelization to picoseconds range
- Study of registers' fault model similar or not?
- Consequences on DFA schemes

Thank you for your attention

Laser benches open for academics on cooperation basis

Bring and test your own device

dutertre@emse.fr