Laser Fault Injection in Microcontrollers

- Laser Fault Injection – How faults happen
- LFI fault models
  - At gate level
  - In MCUs
  - Multiple faults

État de l’art des modèles de faute sur microcontrôleur

Projet Forward

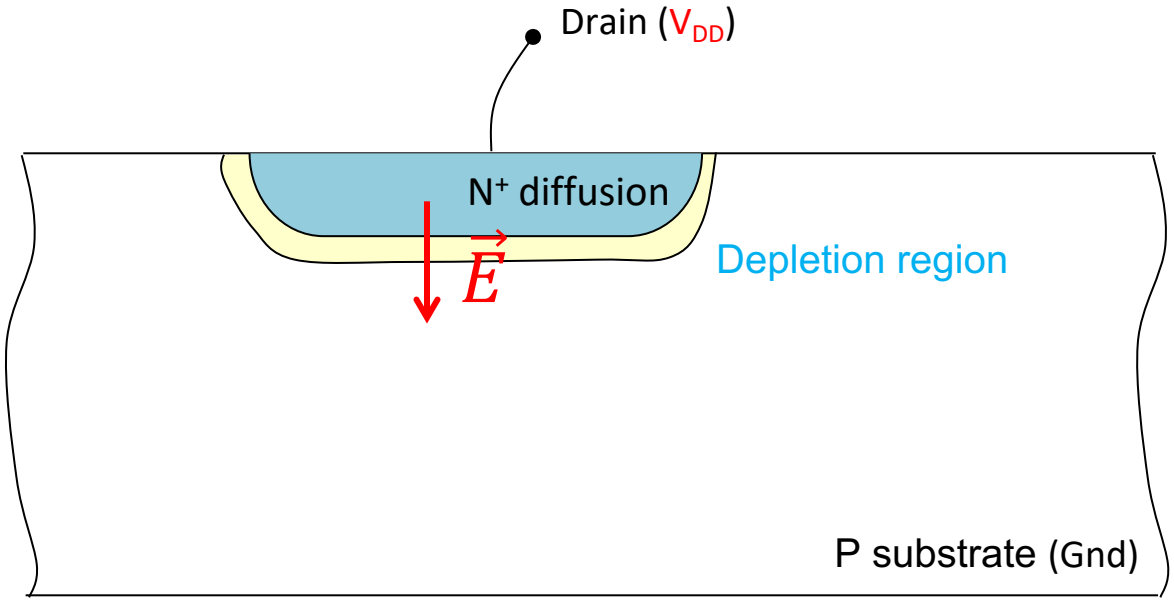
Lundi 30 mars 2026

Jean-Max Dutertre IMT/MSE

LFI – How faults happen

- From transient current generation …

- Reverse biased PN junction → electric field

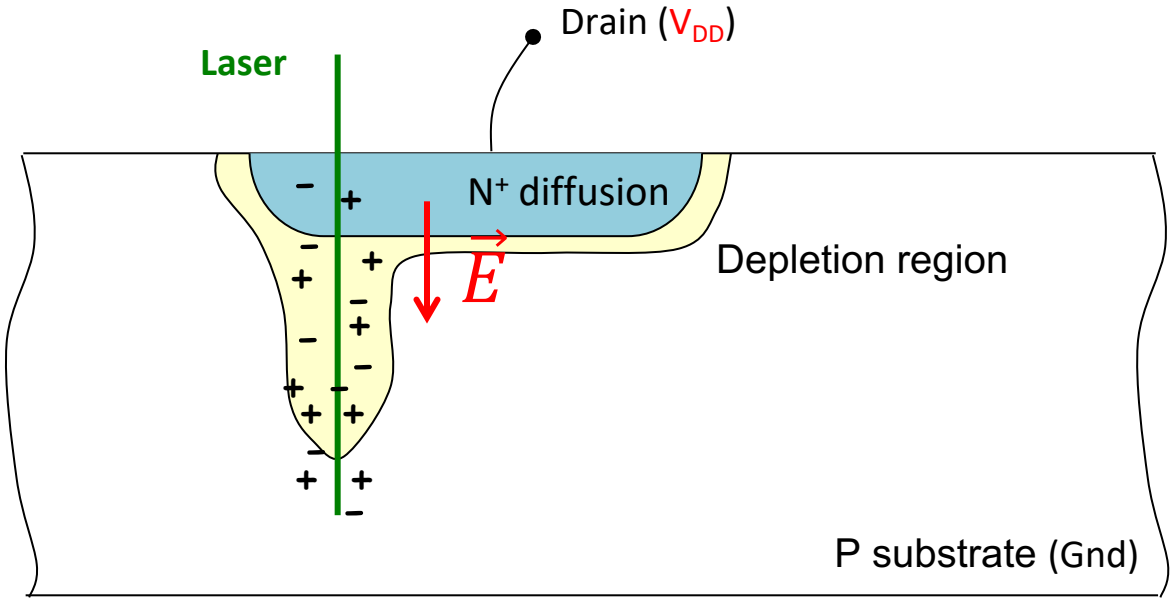


LFI – How faults happen

- From transient current generation …

- Laser-induced charge carriers are put into motion

→ A transient current is induced

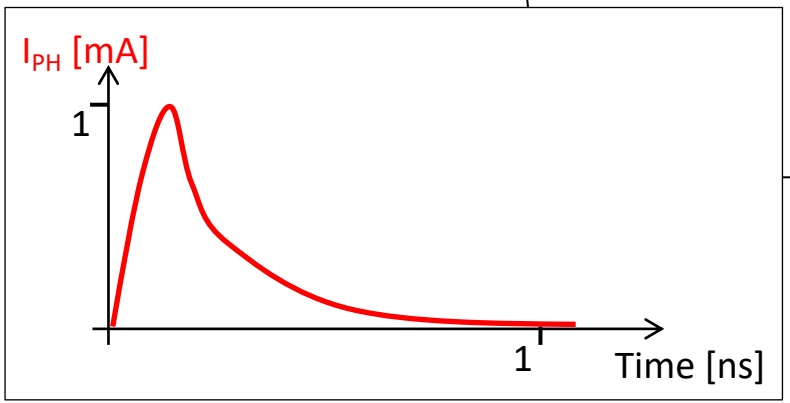


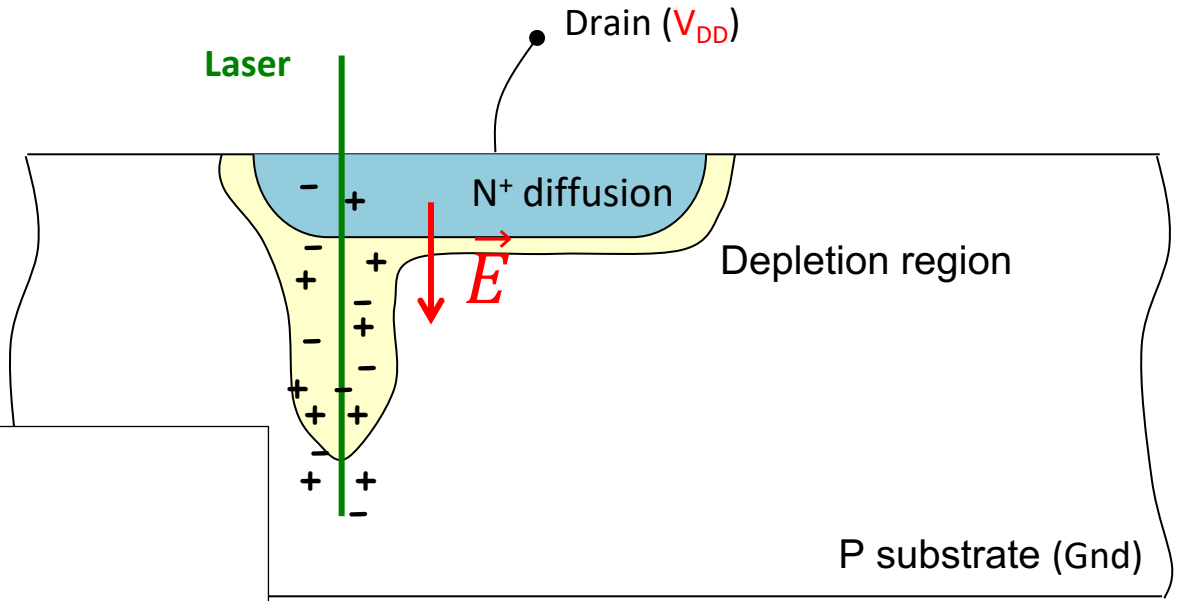
LFI – How faults happen

- From transient current generation …

- Laser-induced charge carriers are put into motion

→ A transient current is induced I_{PH}

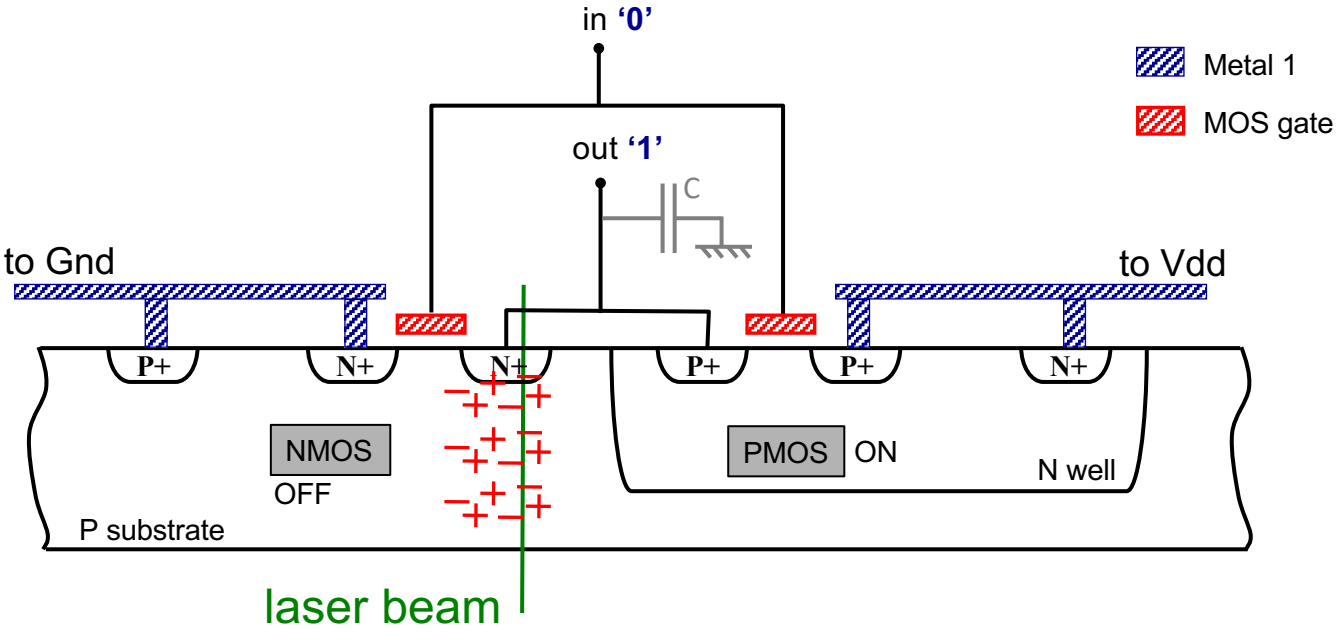




⇨ Reverse biased PN junction = laser sensitive parts of an IC

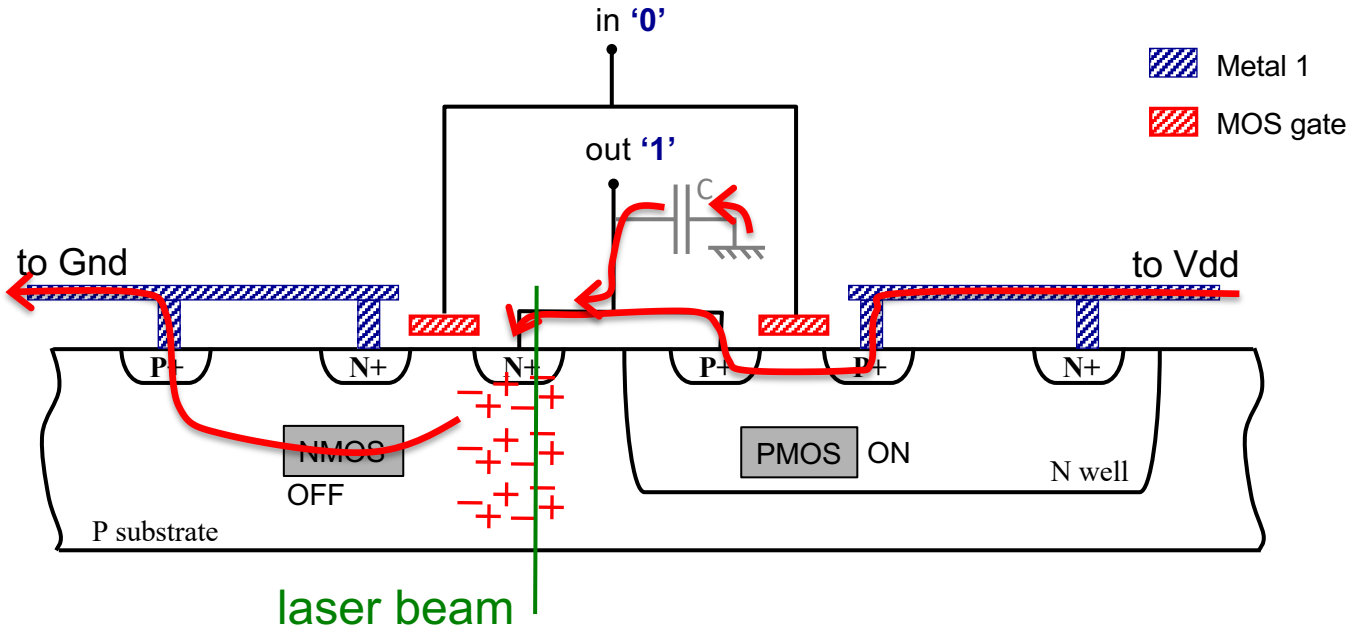
LFI – How faults happen

- … to voltage transient …



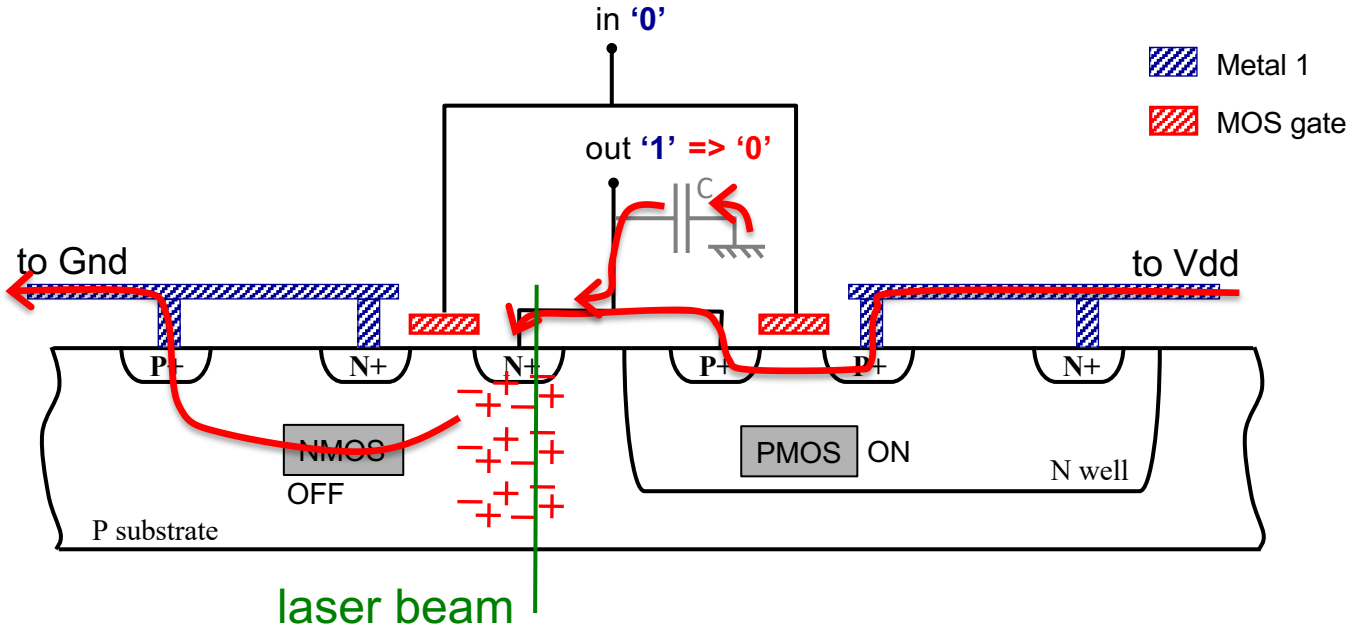
LFI – How faults happen

- … to voltage transient …



LFI – How faults happen

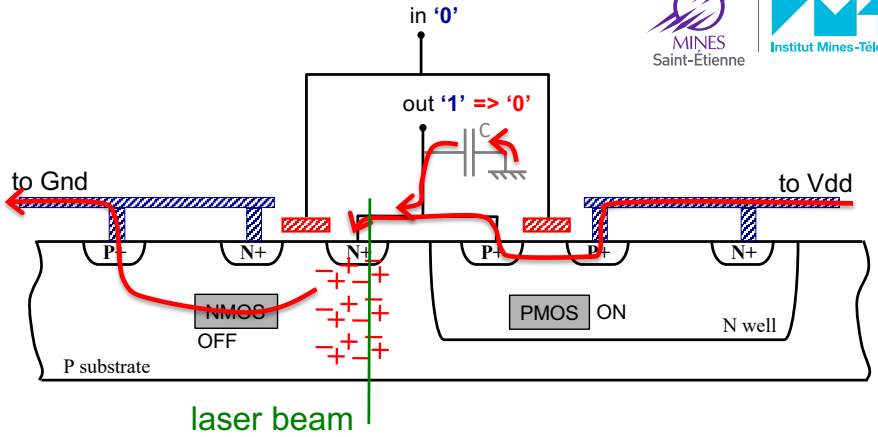
- … to voltage transient …

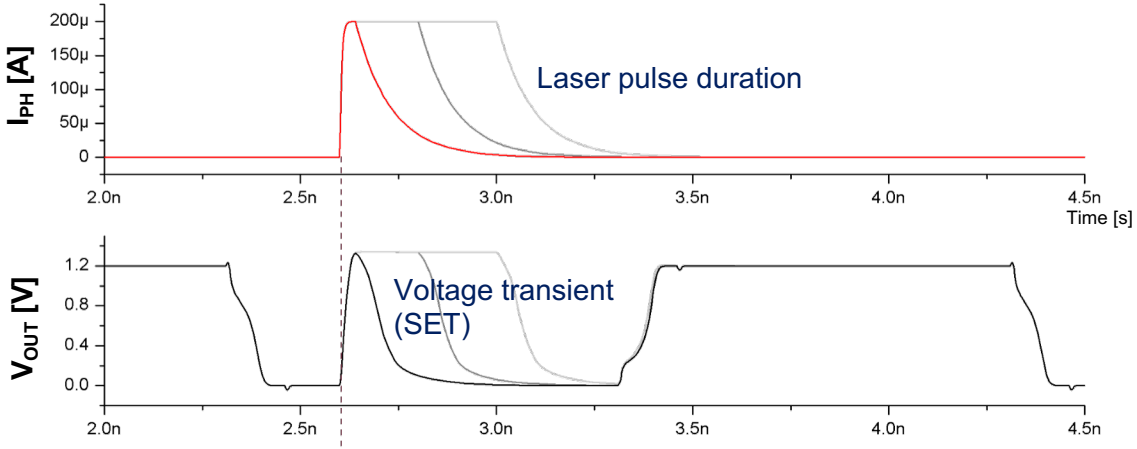


⇨ Drains of OFF CMOS transistors = laser sensitive parts of an IC

LFI – How faults happen

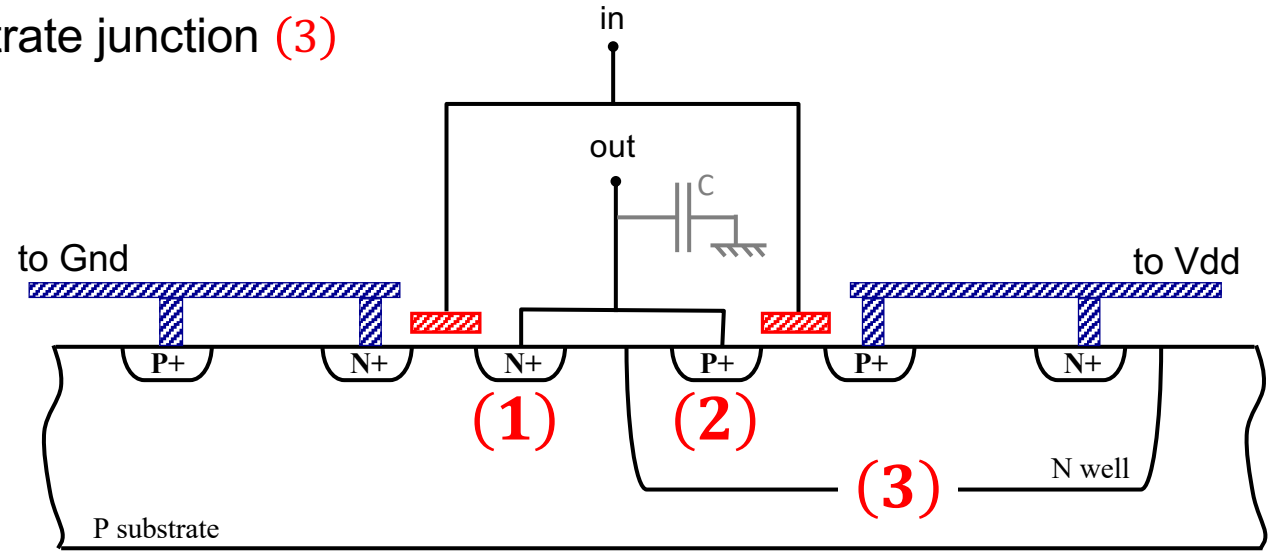
- … to voltage transient …





LFI – How faults happen in CMOS bulk devices

- LFI sensitive POIs → reverse biased PN junctions
  - ✓ NMOS/PMOS drain (1)/(2)
  - ✓ Nwell - Psubstrate junction (3)



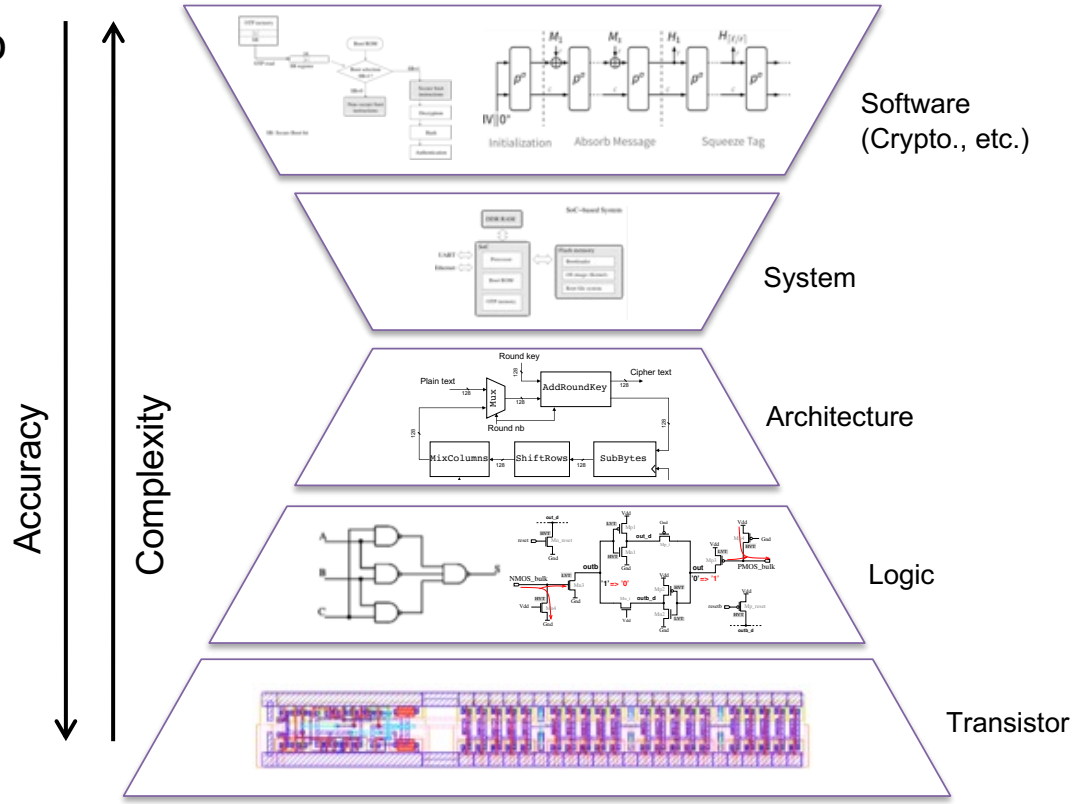
Laser Fault Injection in Microcontrollers

- Laser Fault Injection – How faults happen
- LFI fault models
  - At gate level
  - In MCUs
  - Multiple faults

LFI fault models

Different level of abstraction to describe faults

- From gate level …
- … to architecture/software level



LFI fault models

- Fault model: characteristics of the injected fault
  - Fault type (mathematical expression) → often called the fault model
  - Fault location
  - Fault timing
  - Fault size (# bits, # bytes, # instructions, etc.)
  - Fault duration
  - Fault repeatability

  - Sometimes requirements to be fulfilled for a given attack
    (e.g. Giraud DFA against AES: single-bit fault before the last SubBytes transformation)

Laser Fault Injection in Microcontrollers

- Laser Fault Injection – How faults happen
- LFI fault models
  - At gate level
  - In MCUs
  - Multiple faults

LFI fault models – At gate level

Fault model: at bit level

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

$$b \xrightarrow{\text{⚡}} \text{not}(b)$$

- Bit-set/reset (data dependent)

$$\left.\begin{array}{l} \text{if } b = 0 \xrightarrow{\text{⚡}} b = 1 \\ \text{if } b = 1 \xrightarrow{\text{⚡}} b = 1 \end{array}\right\} \text{Bit-set}$$

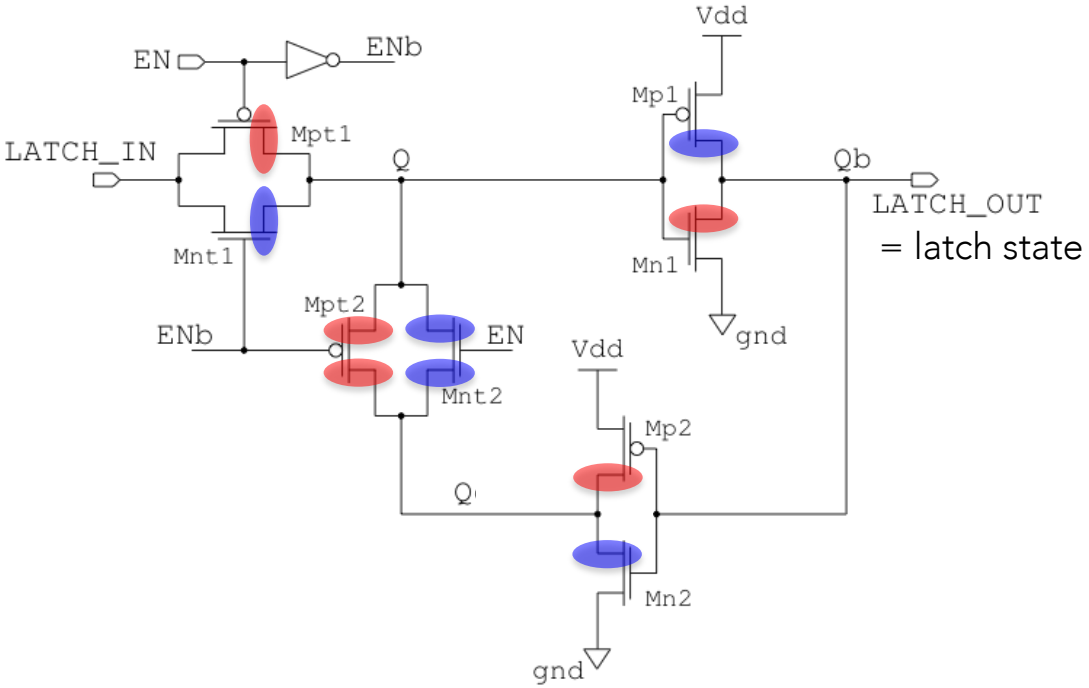
$$\left.\begin{array}{l} \text{if } b = 0 \xrightarrow{\text{⚡}} b = 0 \\ \text{if } b = 1 \xrightarrow{\text{⚡}} b = 0 \end{array}\right\} \text{Bit-reset}$$

Provide additional information on the original bit value

→ Safe error attack

Experimental results – Memory cells

- LFI in D-latch (half register) – Schematic

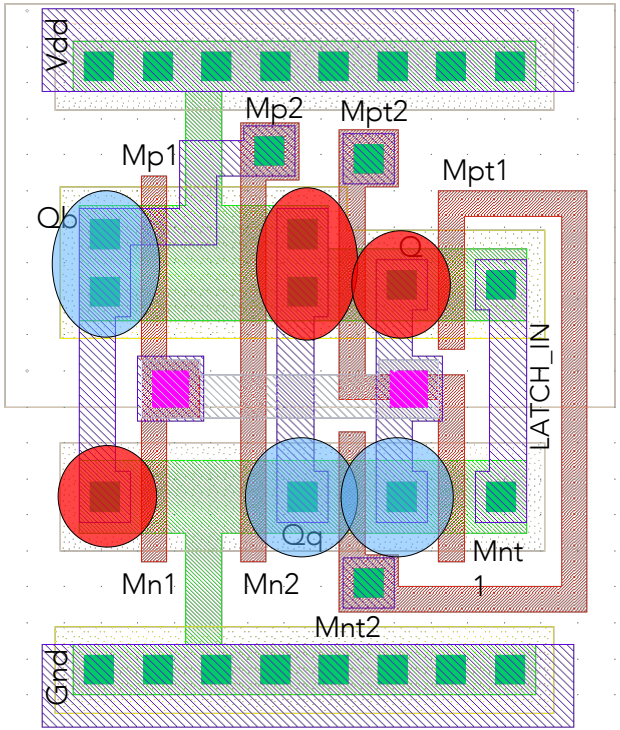


Bit-set sensitive area

Bit-reset sensitive area

Experimental results – Memory cells

- LFI in D-latch (half register) – Layout

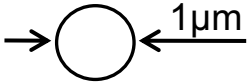


Metal 1
MOS gate
Diffusion

Bit-set sensitive area

Bit-reset sensitive area

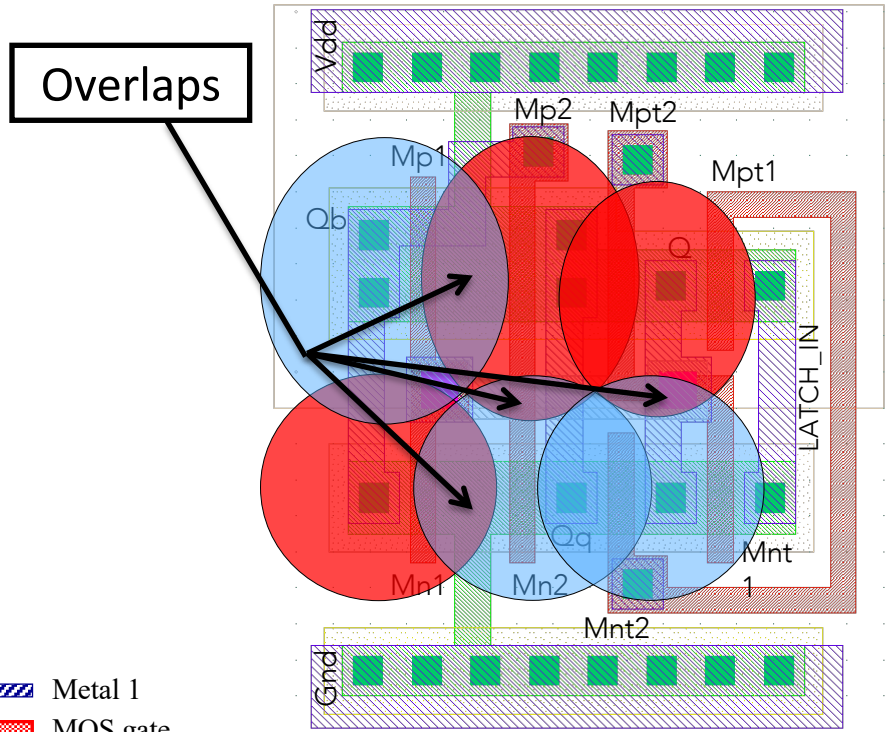
Laser spot size/effect area:



- Depending of the targeted area:
  - Bit-set FM
  - Bit-reset FM
  - Single-bit fault

Experimental results – Memory cells

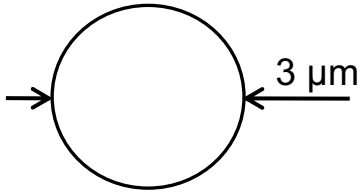
- LFI in D-latch (half register) – Layout



Bit-set sensitive area

Bit-reset sensitive area

Laser spot size/effect area:

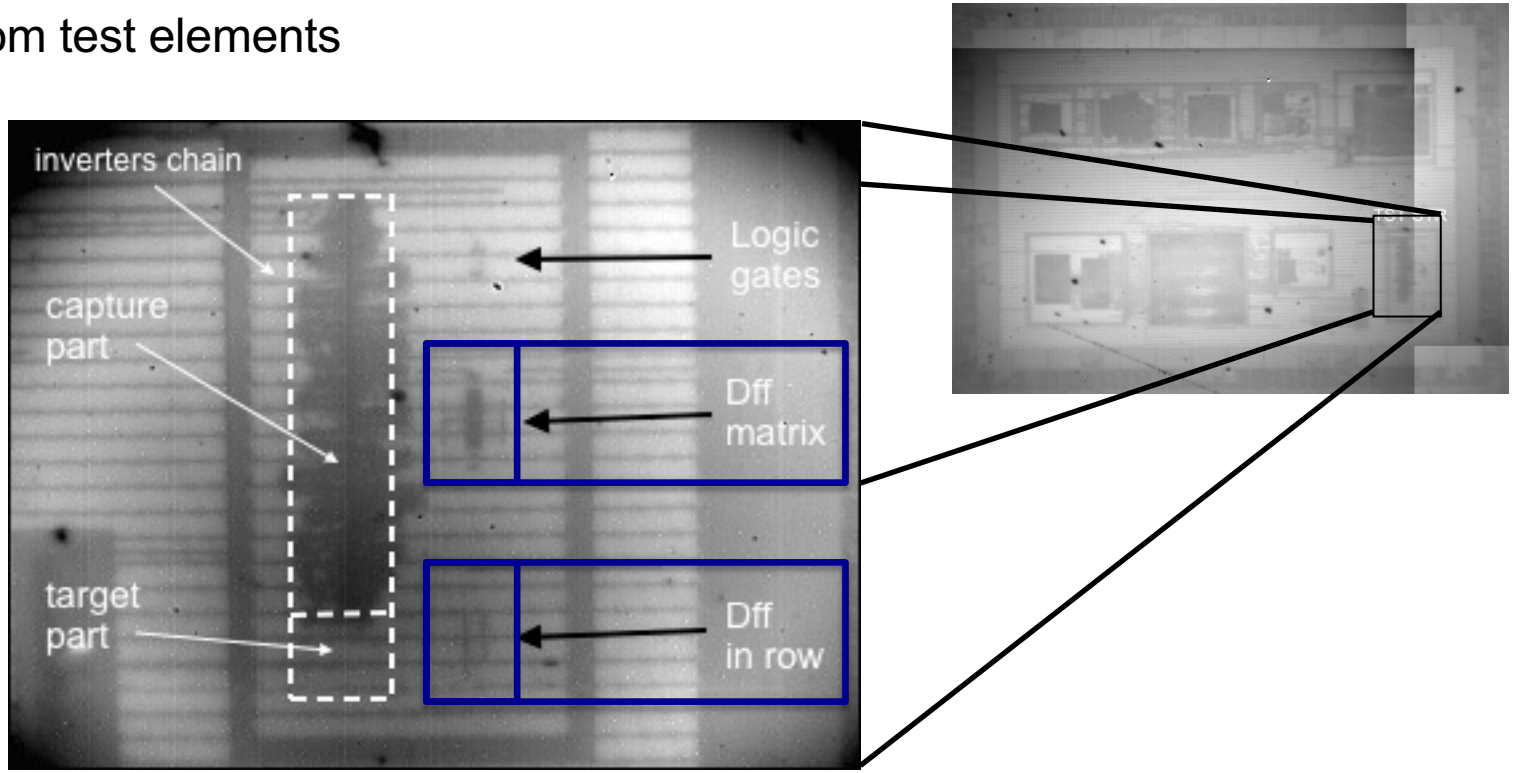


- Overlap of laser sensitive areas
  - Bit-flip-fault model?
  - Question the bit-set/Reset FM?

Experimental results – Memory cells

- DFF at the CMOS 28 nm technology node

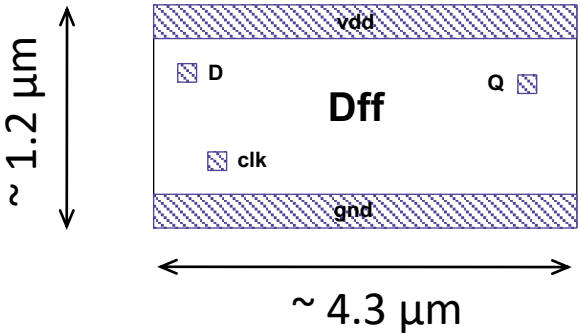
Custom test elements

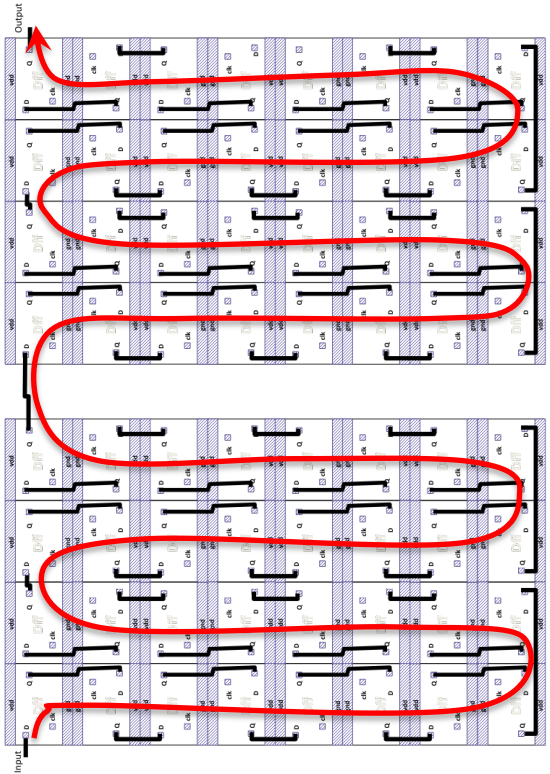


Experimental results – Memory cells

- DFF at the CMOS 28 nm technology node

Matrix shaped shift register with 64 D flip-flops



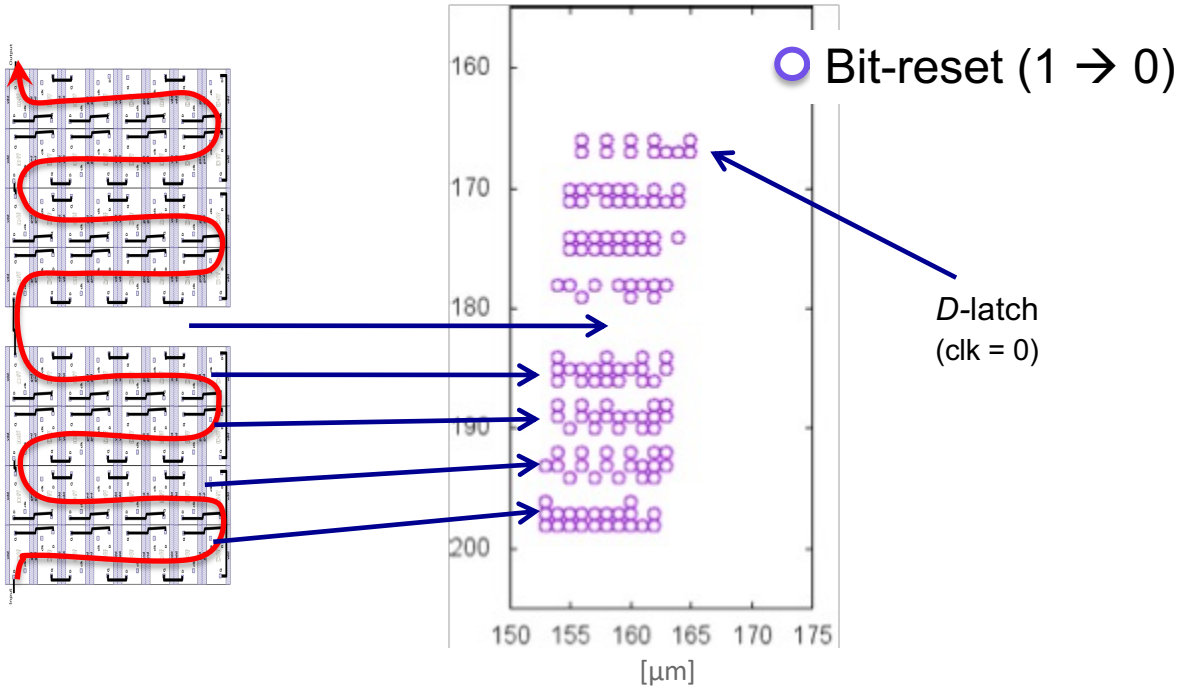


- DFF: ~ 40 transistors
- Large output buffer

Experimental results – Memory cells

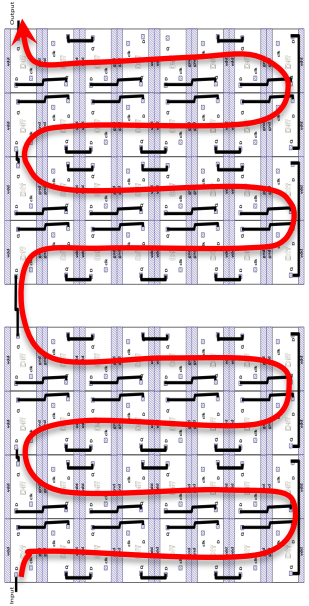
- DFF at the CMOS 28 nm technology node

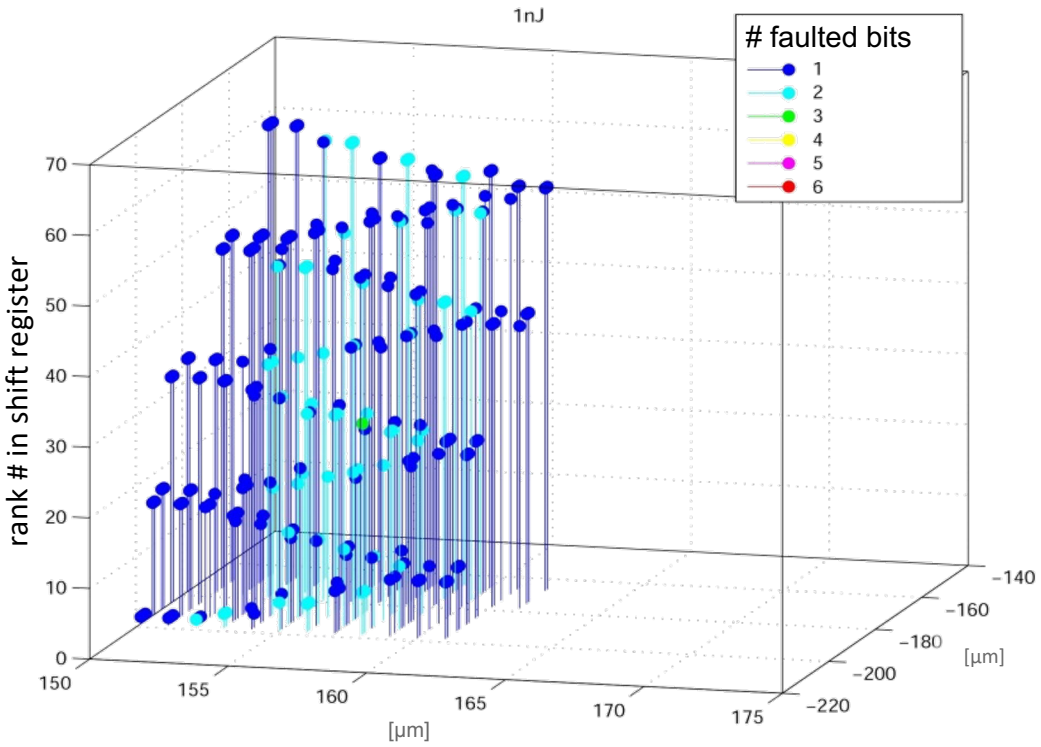
Static LFI – Parameters: 1 µm spot / **30 ps** / 0.5 nJ / Δxy = 1 µm



Experimental results – Memory cells

3D view at 1 nJ

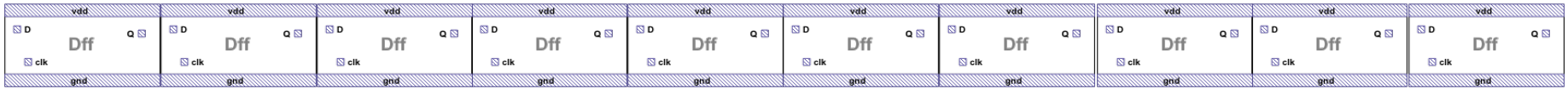




Experimental results – Memory cells

- DFF at the CMOS 28 nm technology node

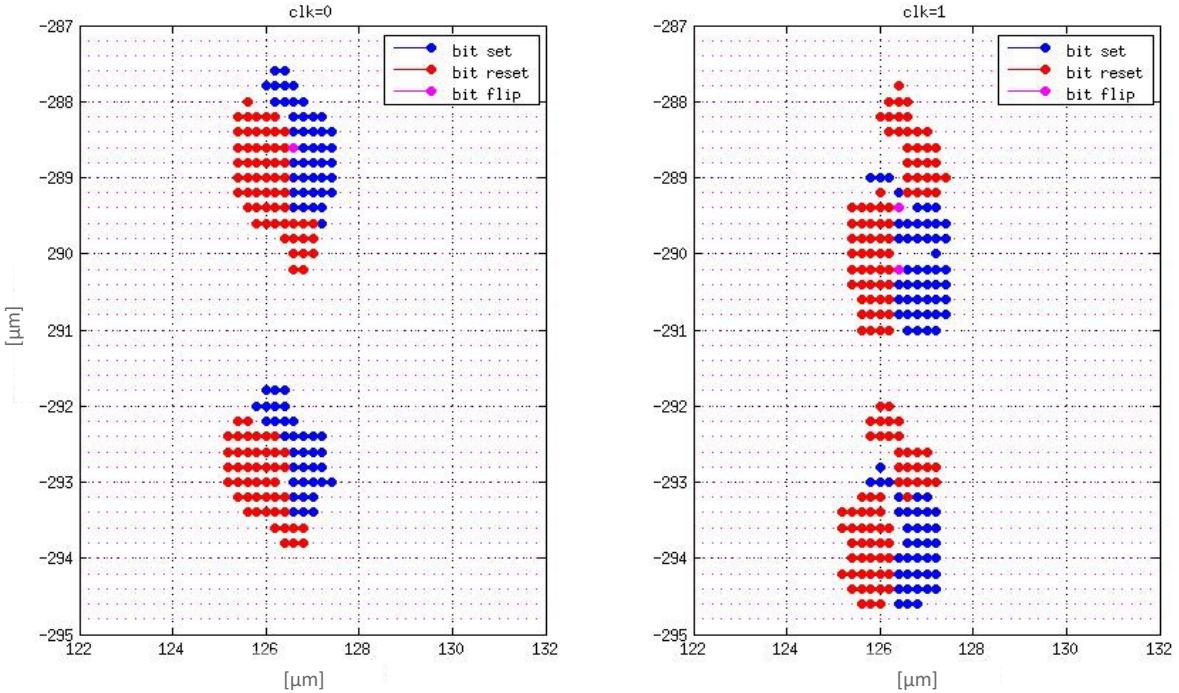
In-line shift register with 10 D flip-flops



Experimental results – Memory cells

- DFF at the CMOS 28 nm technology node

Static LFI – Parameters: 1 µm spot / 30 ps / 0.5 nJ / Δxy = 0.2 µm / backside

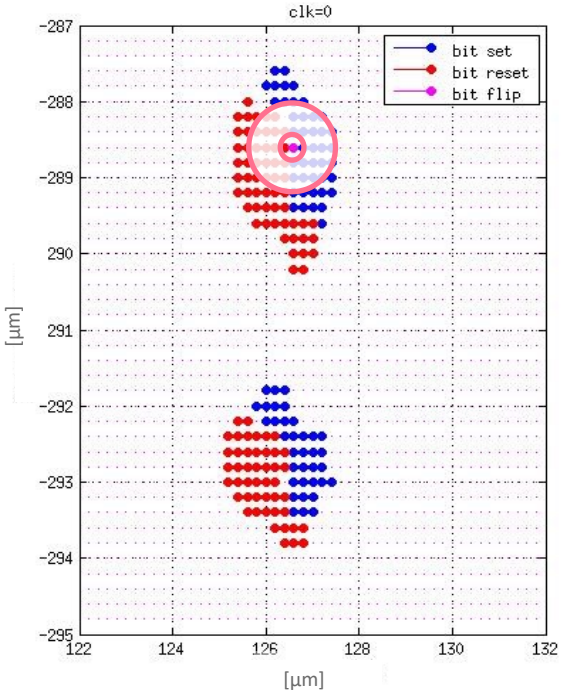


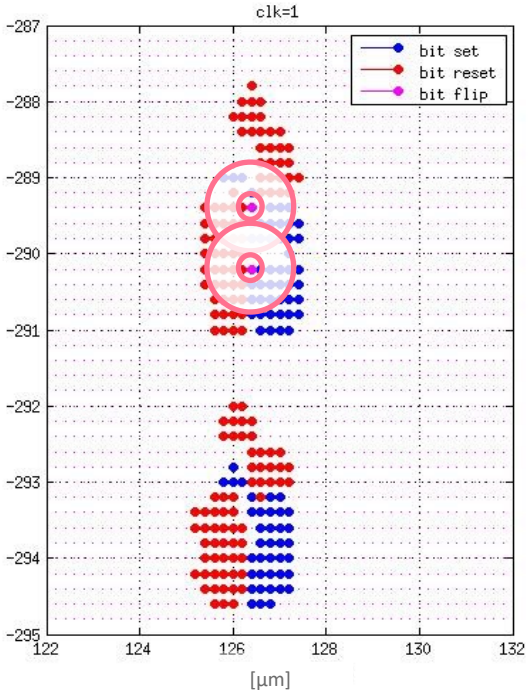
Experimental results – Memory cells

- DFF at the CMOS 28 nm technology node

Static LFI – Parameters: 1 µm spot / 30 ps / 0.5 nJ / Δxy = 0.2 µm / backside

Bit-flip





Experimental results – Memory cells

- DFF at the CMOS 28 nm technology node

Single-bit + bit-set/reset fault model experimentally assessed

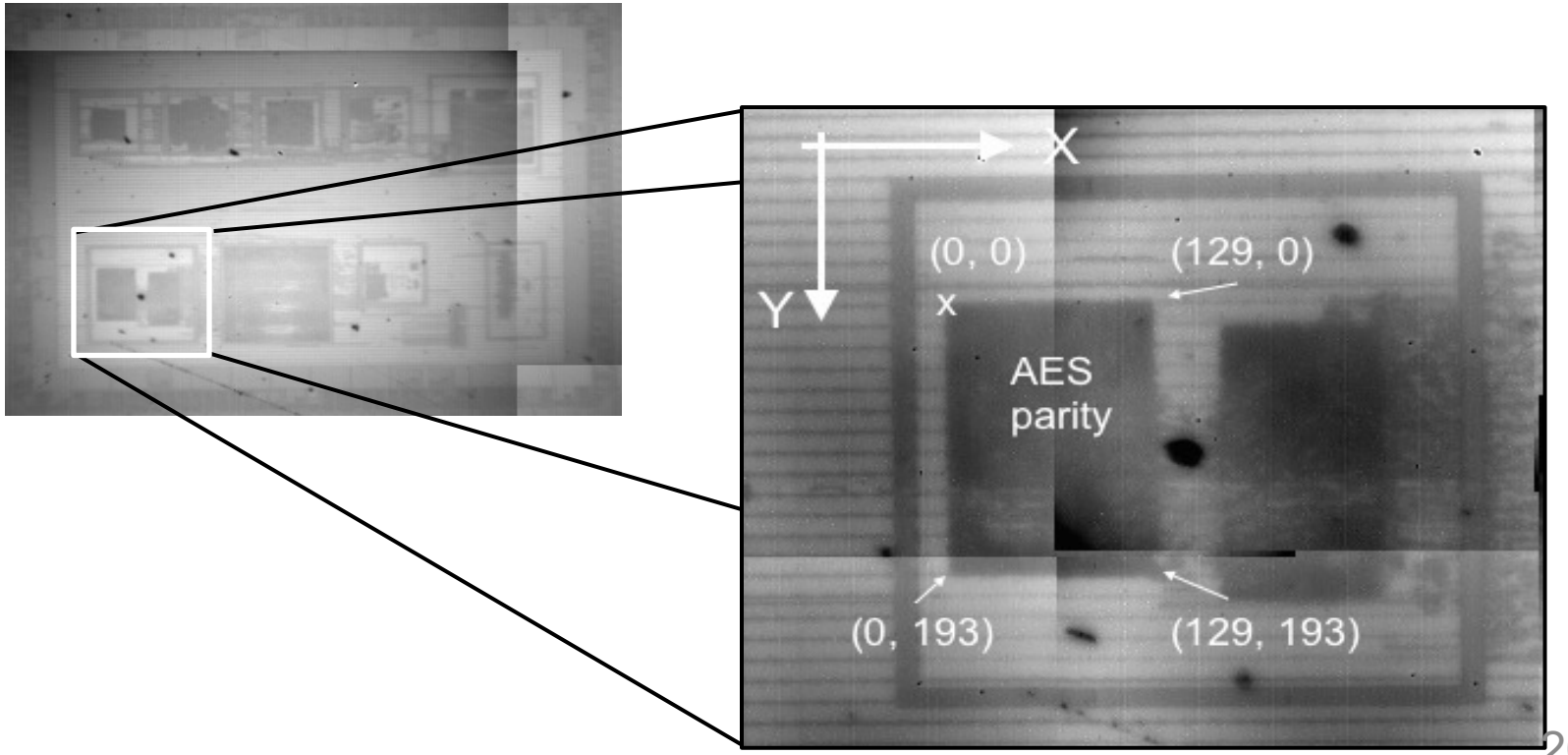
Laser spot 1 µm and 5 µm (see table below)

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

Laser fault injection at the CMOS 28 nm technology node: an analysis of the fault model, J.-M. Dutertre et al., FDTC 2018

Experimental results – Cryptographic accelerator

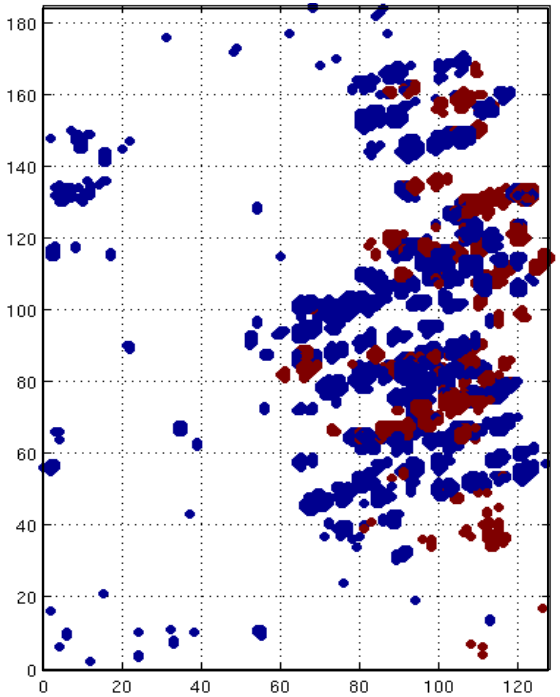
- Hardware AES-128, CMOS 28 nm, V_{DD} = 1.2V, 100 MHz



Experimental results – Cryptographic accelerator

- Hardware AES-128, CMOS 28 nm, V_{DD} = 1.2V, 100 MHz

Dynamic LFI – Parameters: 5 µm spot / 10 ns / 0.6-1.0 W / Δxy = 1µm / backside / AES 9th round



26,380 faulted cipher texts

- Unidentified faults

6,574 (24.9%)

faulted bytes: 5 – 8

- Identified faults

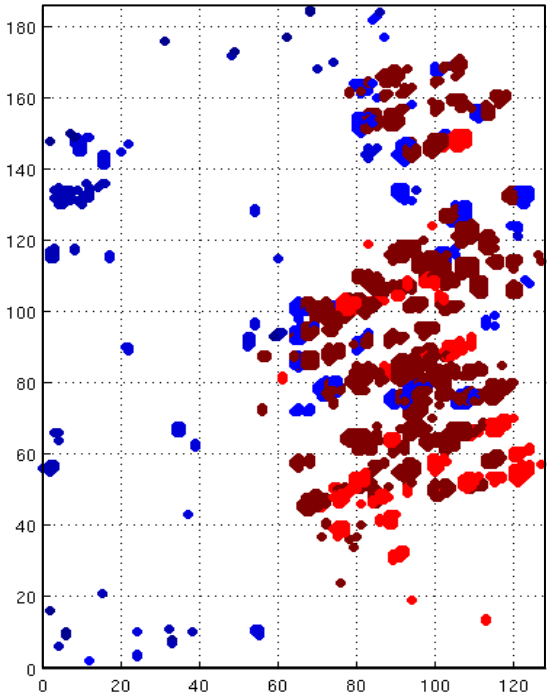
19,806

Mostly single-byte faults

Experimental results – Cryptographic accelerator

- Hardware AES-128, CMOS 28 nm, V_{DD} = 1.2V, 100 MHz

Dynamic LFI – Parameters: 5 µm spot / 10 ns / 0.6-1.0 W / Δxy = 1µm / backside / AES 9th round



- Key schedule (round key computation)

16,253 (61.6 %)

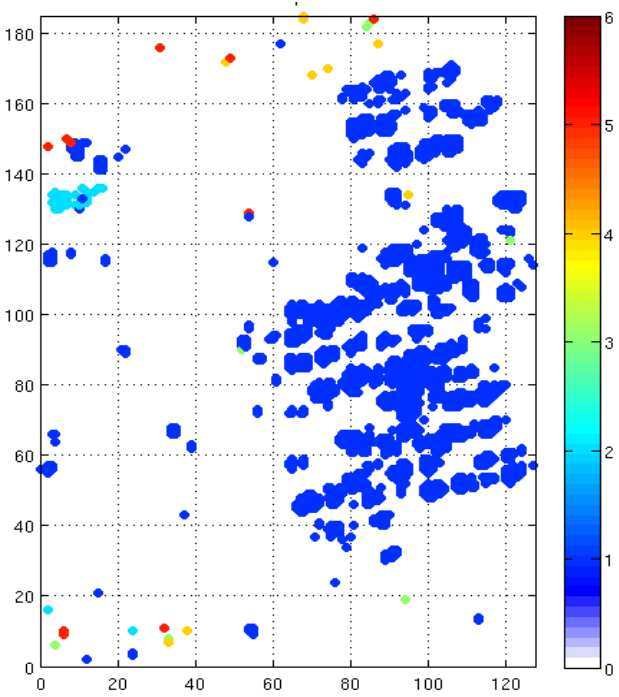
- Datapath

3,553 (13.5 %)

Experimental results – Cryptographic accelerator

- Hardware AES-128, CMOS 28 nm, V_{DD} = 1.2V, 100 MHz

Dynamic LFI – Parameters: 5 µm spot / 10 ns / 0.6-1.0 W / Δxy = 1µm / backside / AES 9th round



Single-byte faults analysis

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

Experimental results – At gate level

- LFI accurate and repeatable (100% success rate)
- In memory cells (SRAM, DFF)
  - Single-bit fault (up to CMOS 28 nm)
  - Bit-set/reset FM (bit-flip also achievable)
  - Consistent with theory
- In a crypto. accelerator (logic gates + DFFs)
  - Single-bit fault (73% rate at CMOS 28 nm with a 5 µm spot)

→ Shall still be the case for more advanced tech. (14nm, 10nm?)

- LFI can target data:
  - In motion (as other FI means, e.g. EM or voltage glitch)
  - At rest (when stored in SRAM or DFF memory)

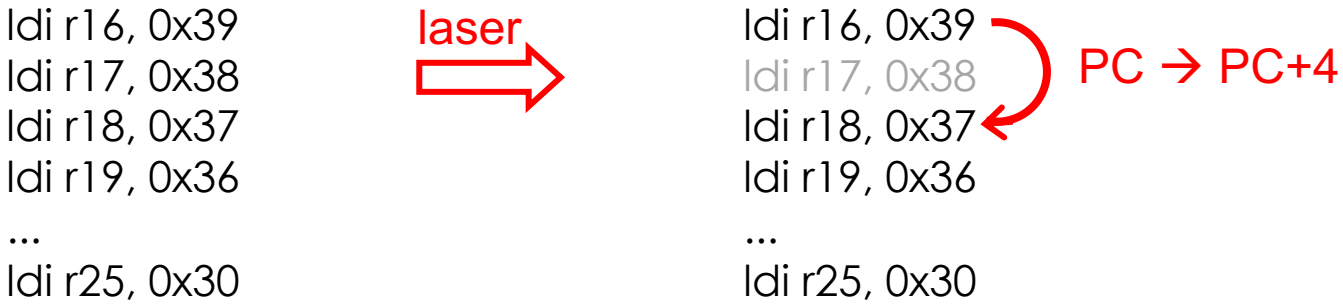
Laser Fault Injection in Microcontrollers

- Laser Fault Injection – How faults happen
- LFI fault models
  - At gate level
  - In MCUs
  - Multiple faults

LFI fault models – In microcontrollers

- The instruction skip fault model

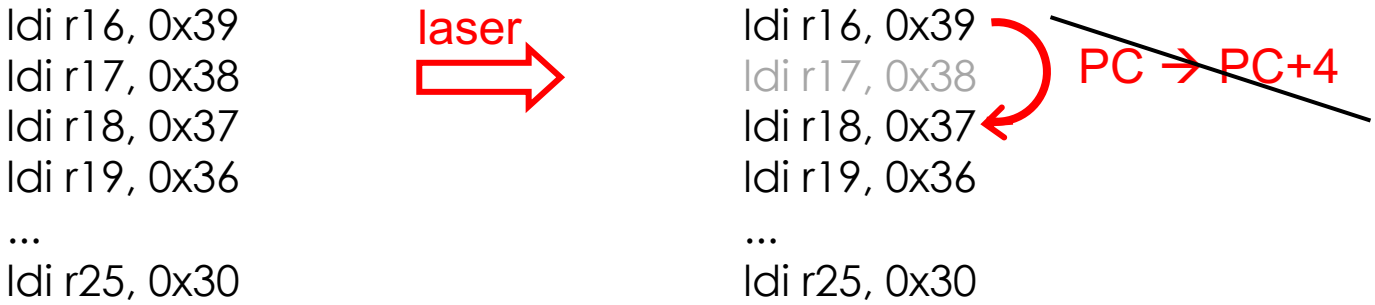
Instruction skip → laser-induced corruption of the Program Counter?



LFI fault models – In microcontrollers

- The instruction skip fault model

Instruction skip → laser-induced corruption of the Program Counter?



- No known LFI in the PC of a microcontroller
- Not to be discarded, probably difficult to control

LFI fault models – In microcontrollers

- The instruction skip fault model

Instruction skip → nop = no operation instruction (discussed more thoroughly later)

```
ldi r16, 0x39          laser          ldi r16, 0x39
ldi r17, 0x38          ⇨              nop
ldi r18, 0x37                         ldi r18, 0x37
ldi r19, 0x36                         ldi r19, 0x36
...                                   ...
ldi r25, 0x30                         ldi r25, 0x30
```

- Most instruction skips are not actual skips (as if the instr. was erased)
- A convenient model to describe LFI in uCTRL (but an inadequate term)

LFI fault models – In microcontrollers

- The instruction skip fault model

Instruction skip → nop = no operation instruction (discussed more thoroughly later)

```
ldi r16, 0x39          laser          ldi r16, 0x39
ldi r17, 0x38          ⇨              nop
ldi r18, 0x37                         ldi r18, 0x37
ldi r19, 0x36                         ldi r19, 0x36
...                                   ...
ldi r25, 0x30                         ldi r25, 0x30
```

- Ability to induce a single instruction skip?

LFI fault models – In microcontrollers

- The instruction skip fault model

Instruction skip → nop = no operation instruction (discussed more thoroughly later)

```
ldi r16, 0x39          laser          ldi r16, 0x39
ldi r17, 0x38      ⇨                  nop
ldi r18, 0x37                         nop
ldi r19, 0x36                         nop
...                                   ...
ldi r25, 0x30                         ldi r25, 0x30
```

- Ability to induce several instruction skips in a row?

LFI fault models – In microcontrollers

- The instruction skip fault model

Instruction skip → nop = no operation instruction (discussed more thoroughly later)

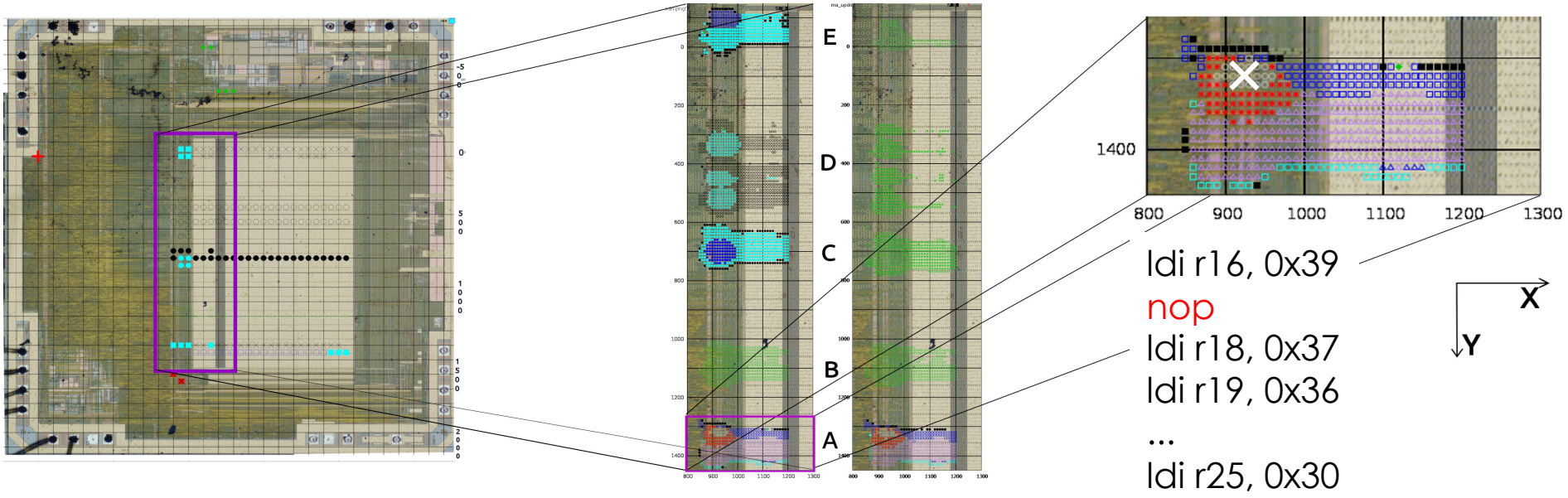
```
ldi r16, 0x39          laser          ldi r16, 0x39
ldi r17, 0x38          ⇨              nop
ldi r18, 0x37                         ldi r18, 0x37
ldi r19, 0x36                         nop
...                                   ...
ldi r25, 0x30                         ldi r25, 0x30
```

- Ability to induce several instruction skips at different times?

Experimental results – Instruction skip FM

- Target: ATmega328P, 8-bit, 16 MHz

LFI parameters: 5 µm spot / 200 ns / 0.4 W / backside

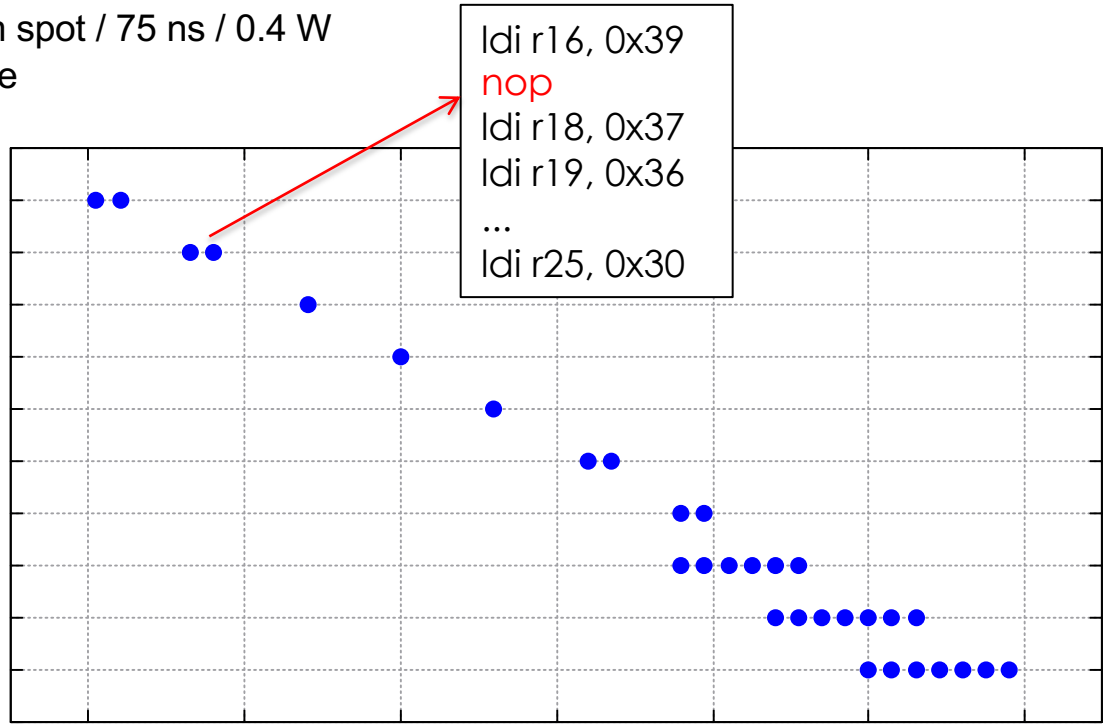


- Exp. basis: laser-induced single instr. skip with 100% repeatability

Experimental results – Instruction skip FM

- LFI – Single instruction skip

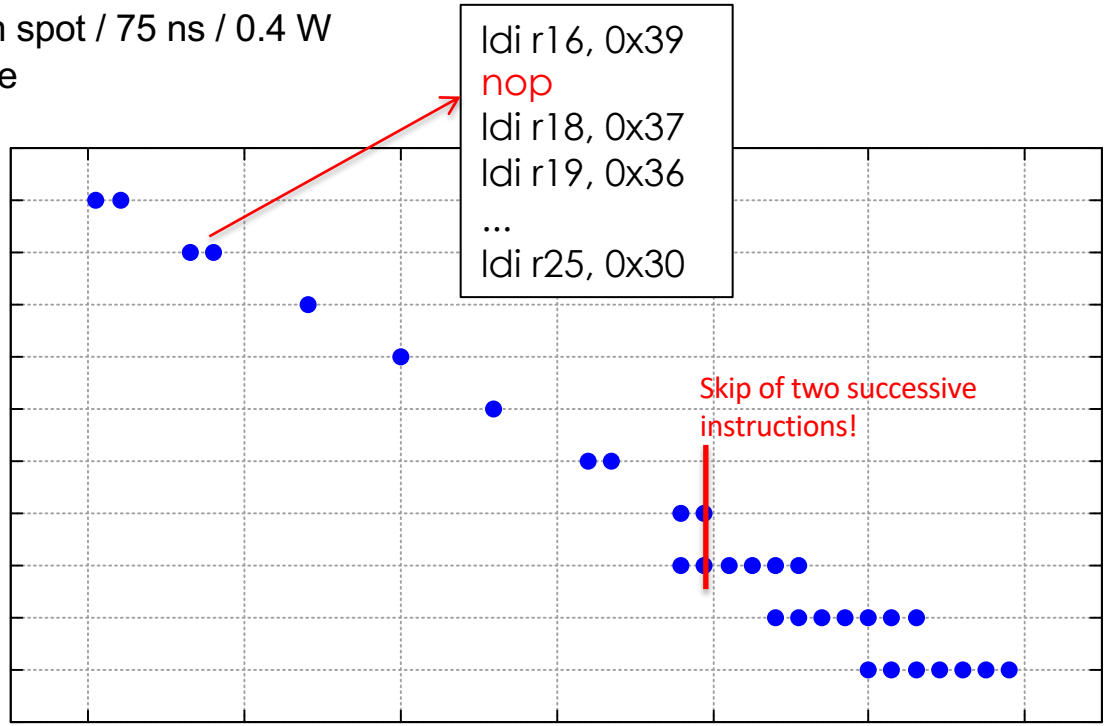
Parameters: 5 µm spot / 75 ns / 0.4 W
100% success rate



Experimental results – Instruction skip FM

- LFI – Single instruction skip

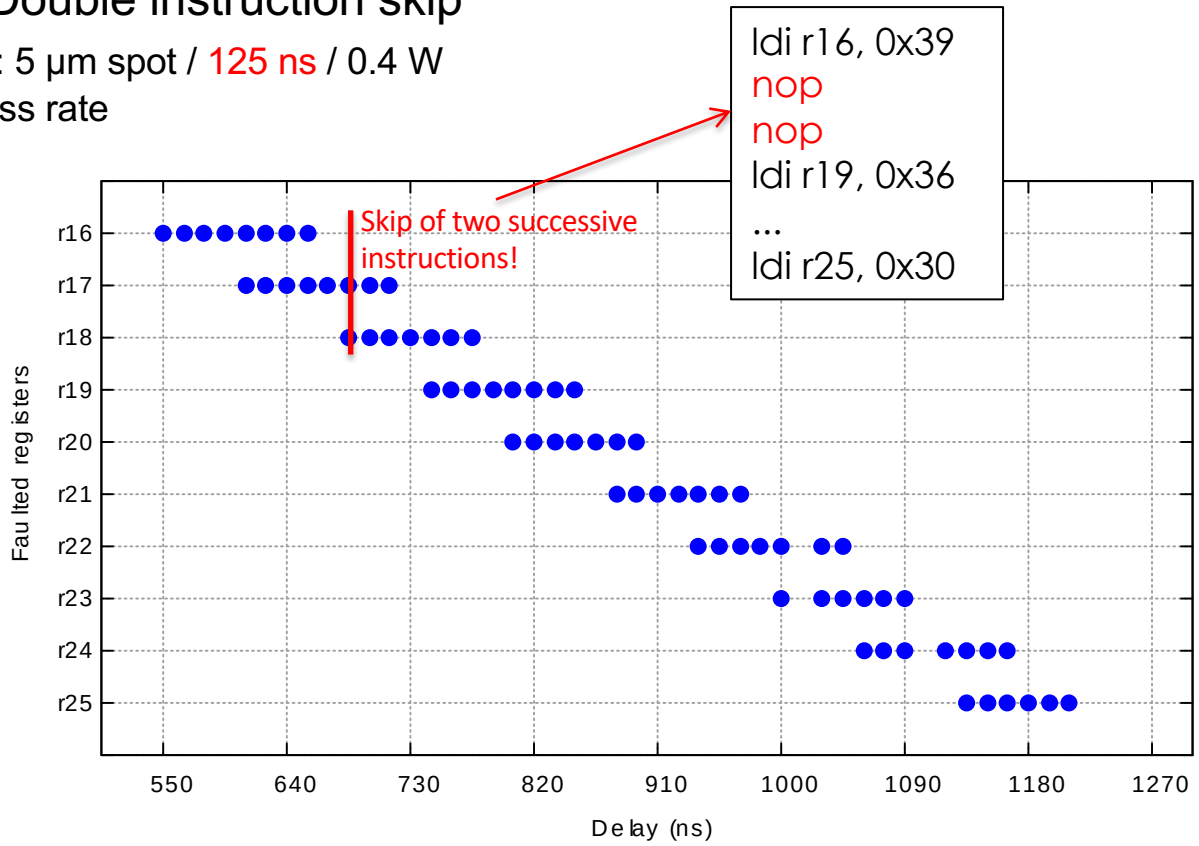
Parameters: 5 µm spot / 75 ns / 0.4 W
100% success rate



Experimental results – Instruction skip FM

- LFI – Double instruction skip

Parameters: 5 µm spot / 125 ns / 0.4 W
100% success rate

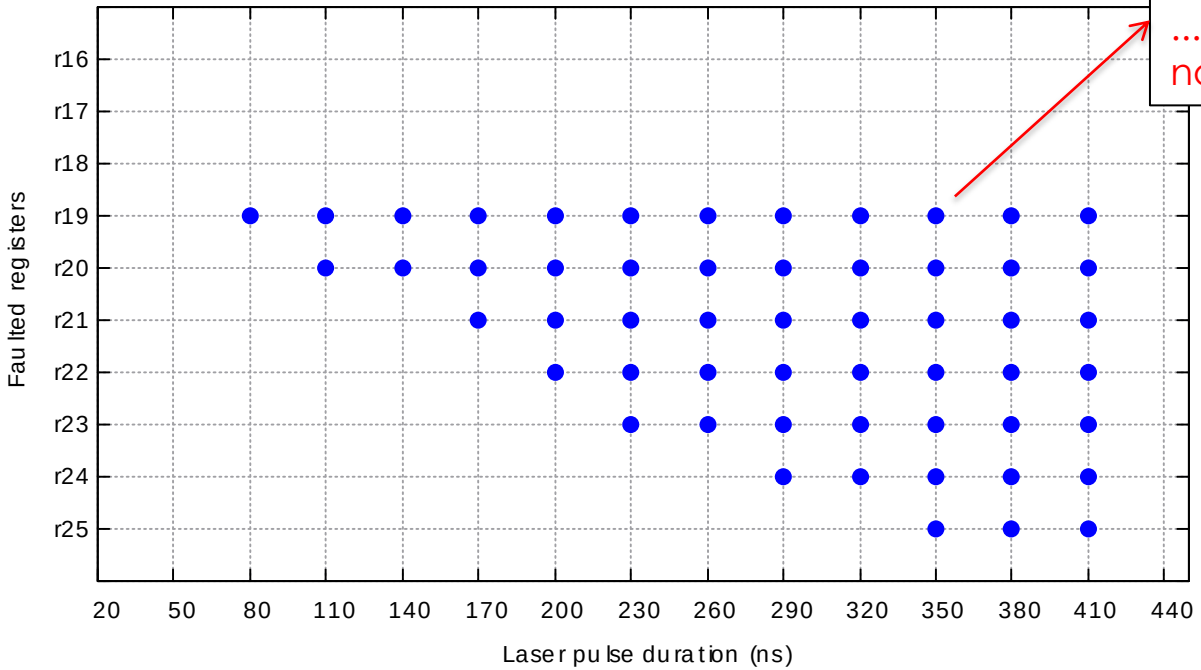


Experimental results – Instruction skip FM

- LFI – Skip of an arbitrary number of instructions

Parameters: 5 µm spot / 80 to 410 ns / 0.4 W
100% success rate

```
ldi r16, 0x39
ldi r17, 0x38
ldi r18, 0x37
nop
...
nop
```



Experimental results – Instruction skip FM

- LFI – Skip of an arbitrary number of instructions

Parameters: 5 µm spot / 50 ns to 20,400 ns / 0.5 W

Laser pulse duration [ns]	1,000	2,000	5,000	10,000	20,400
Number of instr. Skips	17	33	82	143	300

Experimental Analysis of the Laser-Induced Instruction Skip Fault Model,
J.-M. Dutertre et al., Nordsec 2019

Experimental results – At software level

- LFI – Skip of several instructions in a PIN verification algorithm

PIN arrays compare loop

```
BOOL diff = BOOL_FALSE
…
For (i=0; I < PIN_SIZE; i++) {
   if (a1[i] != a2[i]) {
      diff = BOOL_TRUE
   }
}
```

User PIN is incorrect

Experimental results – At software level

- LFI – Skip of several instructions in a PIN verification algorithm

PIN arrays compare loop

```
BOOL diff = BOOL_FALSE
…
For (i=0; I < PIN_SIZE; i++) {
   if (a1[i] != a2[i]) {
      diff = BOOL_TRUE
   }
}
```

User PIN is incorrect

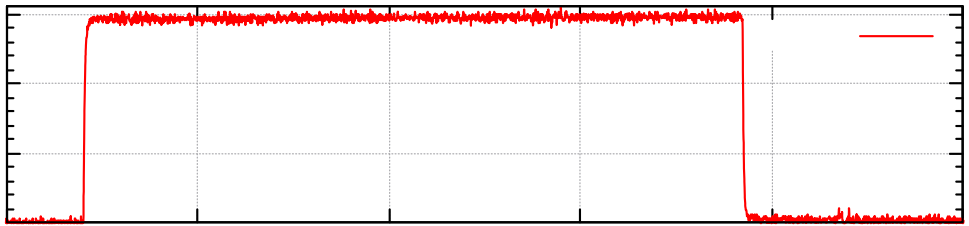
4 separate laser pulses

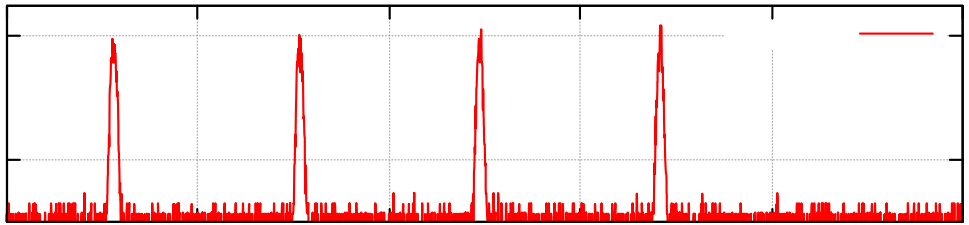
```
BOOL diff = BOOL_FALSE
…
For (i=0; I < PIN_SIZE; i++) {
   if (a1[i] != a2[i]) {
      nop
   }
}
```

Experimental results – At software level

- LFI – Skip of several instructions in a PIN verification algorithm

Parameters: 5 µm spot / 4x 60 ns, 875 ns between pulses / 0.5 W
100% success rate - PIN bypass

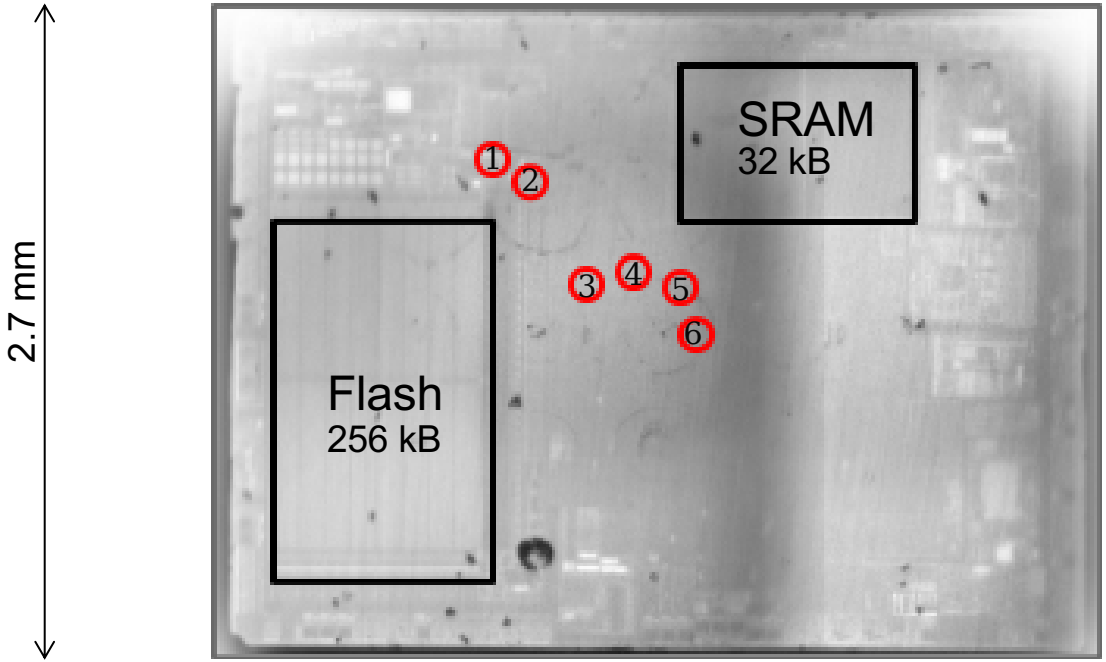




Experimental Analysis of the Laser-Induced Instruction Skip Fault Model, J.-M. Dutertre et al., Nordsec 2019

LFI in the instruction pipeline

- Practical FM – Side effect of the target's microarchitecture
- Target: 32-bit uCTRL, SAMD21, ARM Cortex-M0+ (2-stage pipeline), 12 MHz

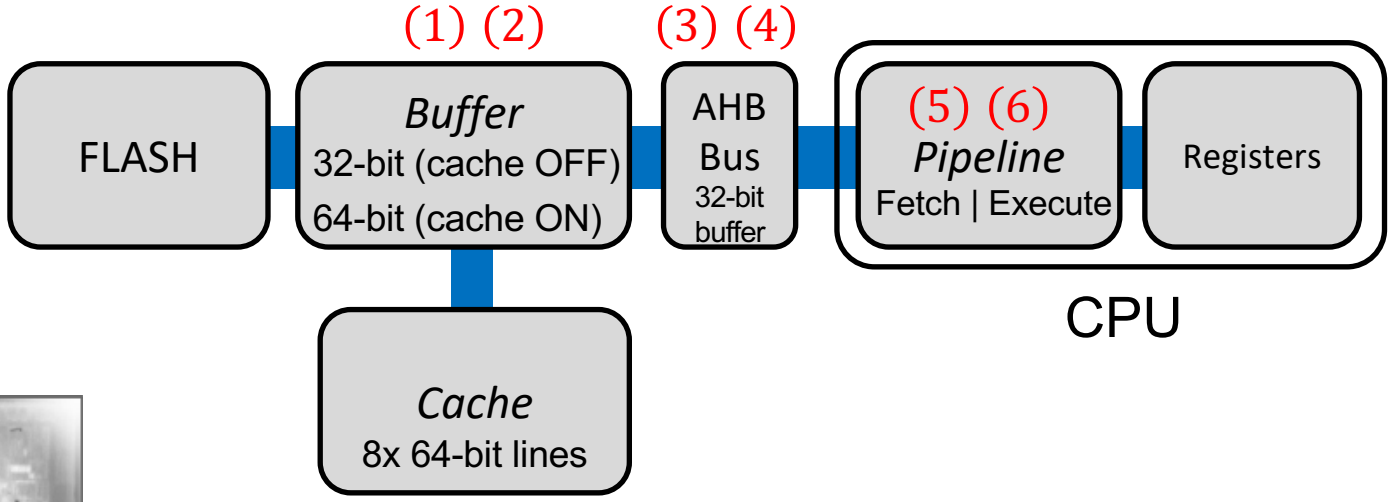


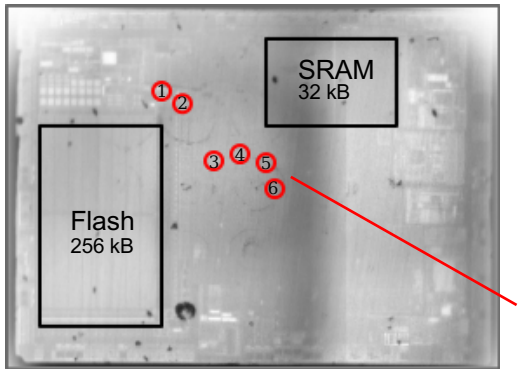
IR camera

LFI in the instruction pipeline

- SAMD21 instruction pipeline

Thumb-2 instructions (mostly 16-bit)



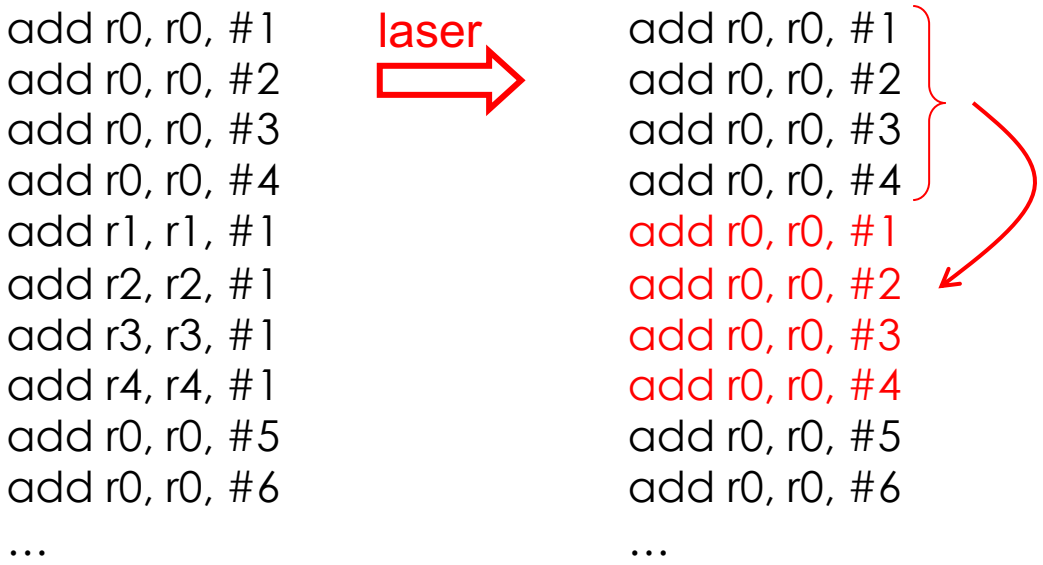


(1) – (6) POI for LFI

LFI in the instruction pipeline

- The instruction replay Fault Model

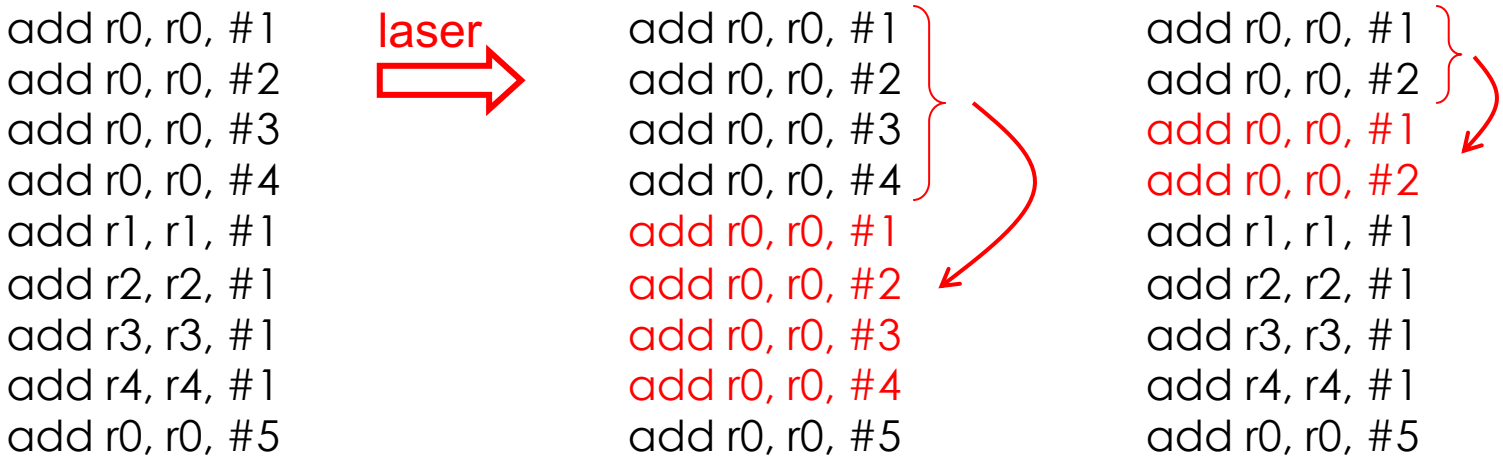
LFI parameters: 20 µm spot / 50 ns / 1.5 W / backside



LFI in the instruction pipeline

- The instruction replay Fault Model

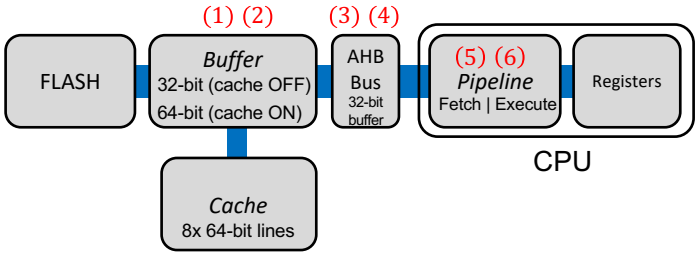
LFI parameters: 20 µm spot / 50 ns / 1.5 W / backside

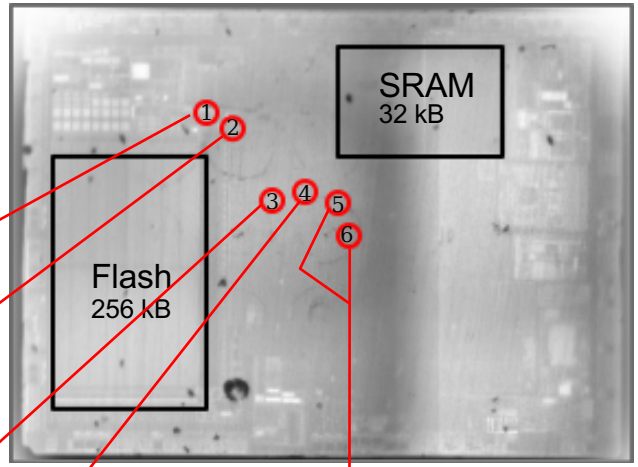


- Replay of 4 (2) instructions for cache ON (OFF) at position (1)
- 4 (2) instructions are overwritten

LFI in the instruction pipeline

- Effect of the target's microarchitecture (and laser spot location)





Replay of 4 (2) instructions

Skip of 4 (2) instructions

Replay of 2 instructions

Skip of 2 instructions

Single-instruction skip

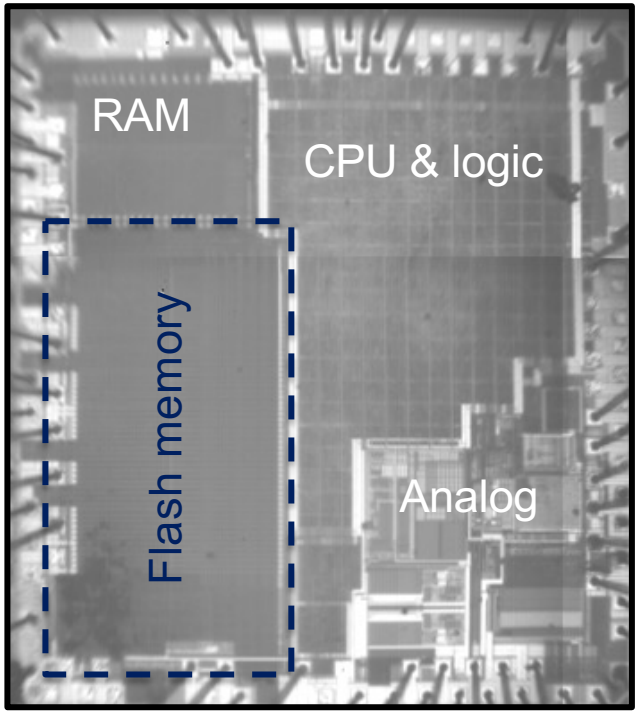
- 100 % success rate

Laser Fault Injection in a 32-bit Microcontroller: from the Flash Interface to the Execution Pipeline, V. Khuat et al., FDTC 2021

Flash memory – LFI at read time

- NOR-Flash: uCTRL embedded NVM

- Firmware storage
- Floating gate transistors
  - ✓ Data storage immune to LFI
- Laser fault injection
  - ✓ **Single-bit**
  - ✓ **Bit-set FM**
  - ✓ At read time
  - ✓ Stored data unmodified



32-bit cortex M3 uCTRL, frontside view, CMOS 90 nm

Flash memory – LFI at read time

- NOR-Flash – LFI exp. results

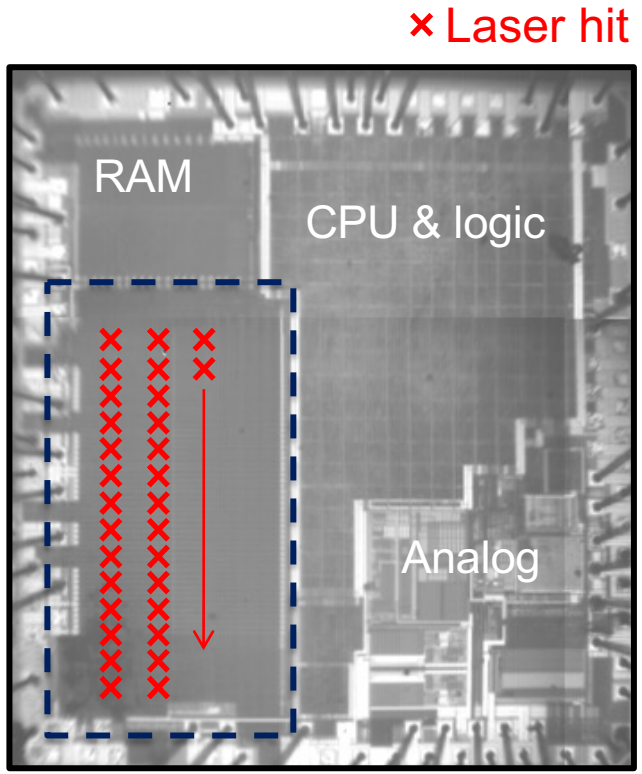
LFI parameters: 5 µm spot / 135 ns / 1 W / backside

- Test code

```
1  test_data:
2  .word 0x00000000
3  NOP
4  LDR R0, test_data
5  NOP
6  # Reading back R0
```

✓ Laser spot: top to bottom

✓ Along vertical lines



32-bit cortex M3 uCTRL, frontside view, CMOS 90 nm

Flash memory – LFI at read time

- NOR-Flash – LFI exp. results

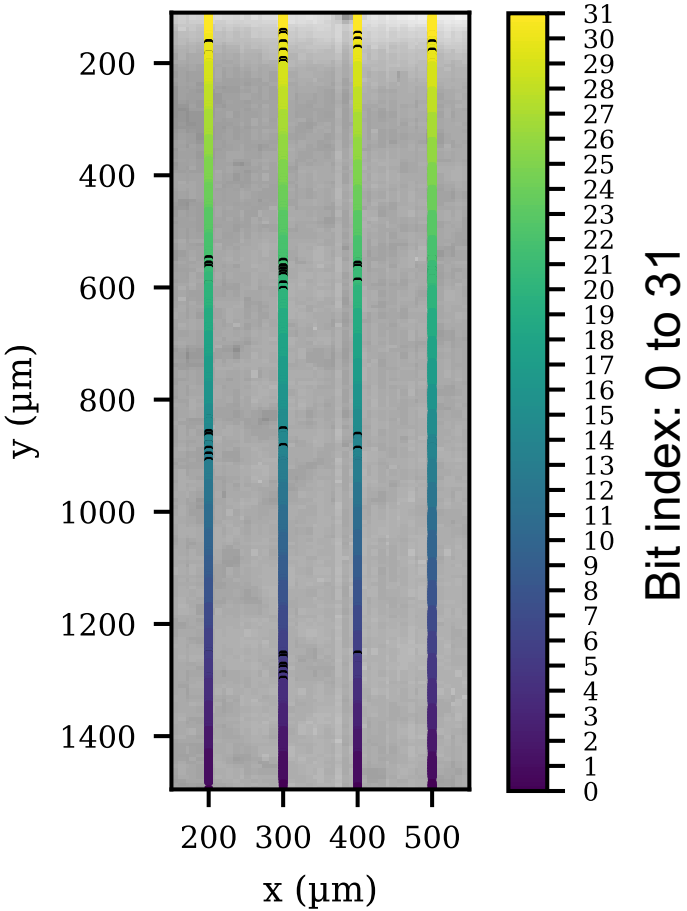
LFI parameters: 5 µm spot / 135 ns / 1 W / backside

- Test code

```
1  test_data:
2  .word 0x00000000
3  NOP
4  LDR R0, test_data
5  NOP
6  # Reading back R0
```

✓ Laser spot: top to bottom

✓ Along vertical lines



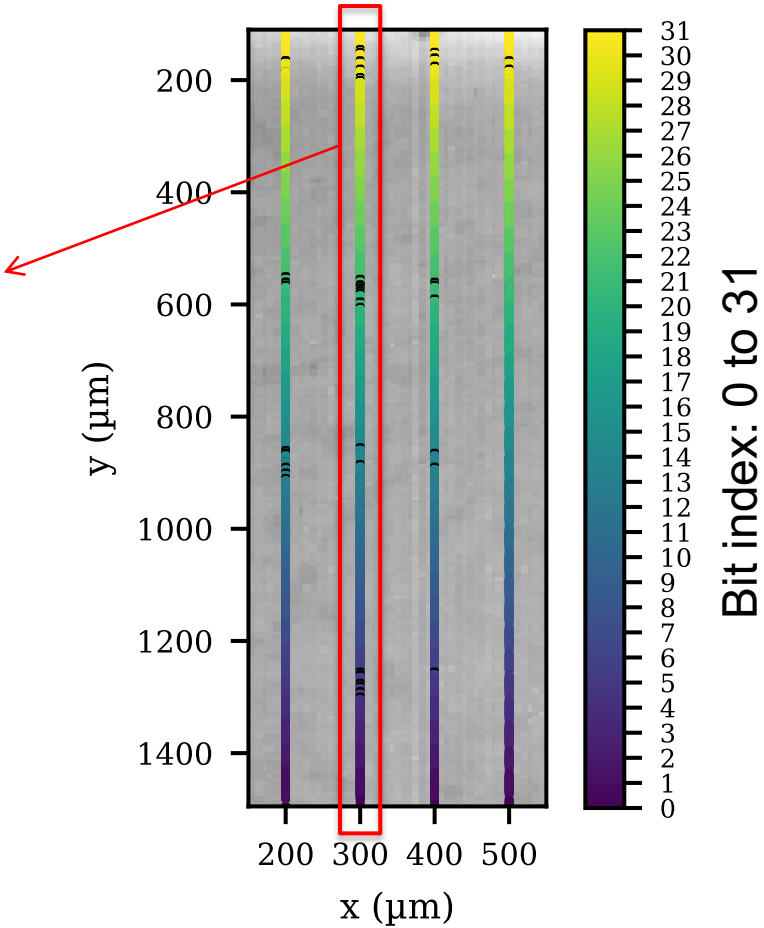
Flash memory – LFI at read time

- NOR-Flash – LFI exp. results

LFI parameters: 5 µm spot / 135 ns / 1 W / backside

Depending on the y position, bits 0 to 31 are faulted

Data/instructions are stored *vertically*



Flash memory – LFI at read time

- LFI at execution time (bit-set FM)
- Targeted instruction: MOVW R0, 0x0000

bits	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Reference instructions																																
Generic MOVW	1	1	1	1	0	i	1	0	0	1	0	0	imm4				0	imm3			Rd				imm8							
MOVW, R0, 0	1	1	1	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

MOVW encoding

Flash memory – LFI at read time

- LFI at execution time (bit-set FM)
- Targeted instruction: MOVW R0, 0x0000

bits	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Reference instructions																																
Generic MOVW	1	1	1	1	0	i	1	0	0	1	0	0	imm4				0	imm3			Rd				imm8							
MOVW, R0, 0	1	1	1	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Data to be written 0x0000

Flash memory – LFI at read time

- LFI at execution time (bit-set FM)
- Targeted instruction: MOVW R0, 0x0000

bits	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Reference instructions																																
Generic MOVW	1	1	1	1	0	i	1	0	0	1	0	0	imm4				0	imm3			Rd				imm8							
MOVW, R0, 0	1	1	1	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Destination register R0

Flash memory – LFI at read time

- LFI at execution time (bit-set FM)
- Targeted instruction: MOVW R0, 0x0000

bits	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Reference instructions																																
Generic MOVW	1	1	1	1	0	i	1	0	0	1	0	0	imm4				0	imm3			Rd				imm8							
MOVW, R0, 0	1	1	1	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Data corruption																																
MOVW, R0, **4**	1	1	1	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0	0	
Destination register corruption																																
MOVW, **R1** 0	1	1	1	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0	0	0	0	0	0	0	
Opcode corruption																																
MOVT, R0, 0	1	1	1	1	0	0	1	0	**1**	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	

Laser-induced Single-bit Faults in Flash Memory: Instructions Corruption on a 32-bit Microcontroller, B. Colombier et al., HOST 2019

Instruction fault models

- LFI practical FMs in microcontrollers

- Instruction skip
  - ✓ Versatile and powerful (from a single-skip to program sections erasure)
  - ✓ Convenient as a model but probably more complex
- Instruction corruption
  - ✓ E.g. LFI in Flash memory
  - ✓ Tailored attacks (breq → brne, etc.)
  - ✓ The “real” instruction skip (out-of-context instructions)
- Instruction replay
  - ✓ Side effect of the micro-architecture
- 100% success rate achievable (linked to time synchronization)

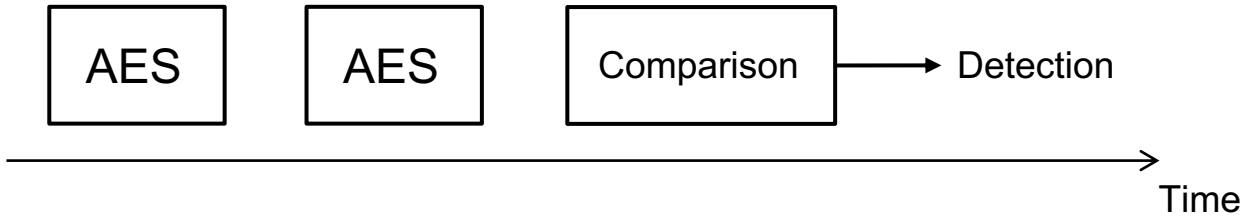
Laser Fault Injection in Microcontrollers

- Laser Fault Injection – How faults happen
- LFI fault models
  - At gate level
  - In MCUs
  - Multiple faults

→ often considered as a means to defeat countermeasures (SW/HW)

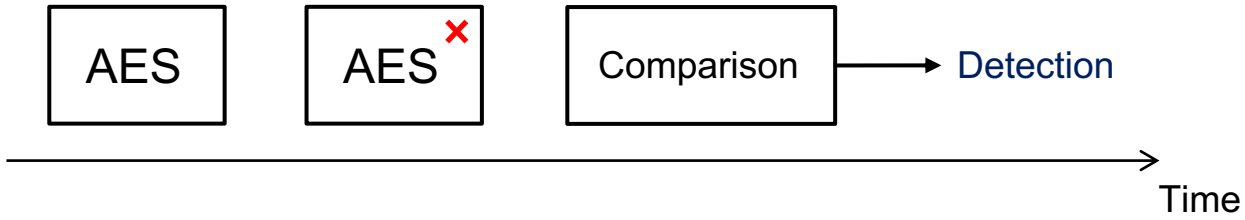
Countermeasures

- Basics – Timing redundancy



Countermeasures

- Basics – Timing redundancy

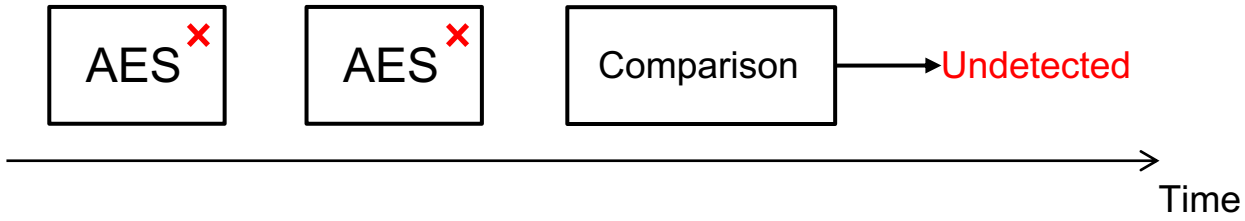


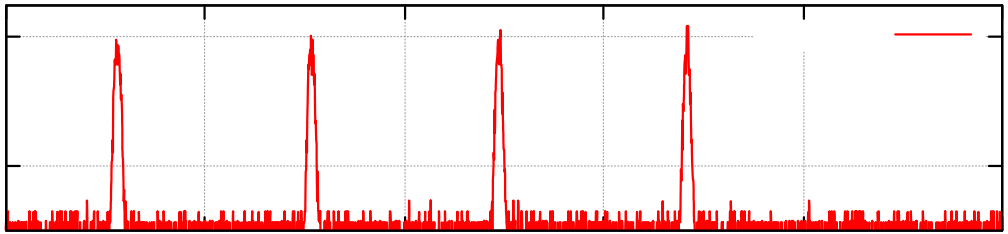
✕ Laser hit

Countermeasures – Multi pulses laser

- Basics – Timing redundancy

→ Multi-pulses laser

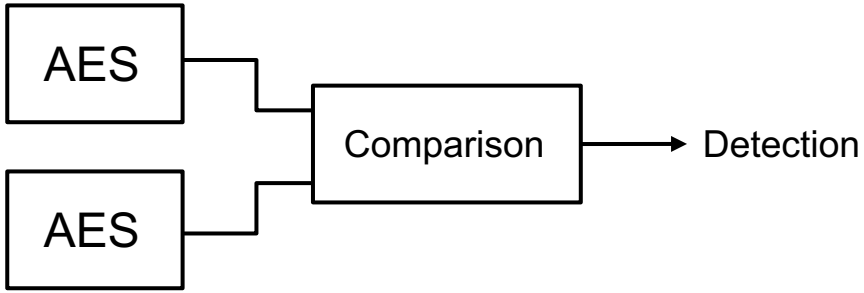




✕ Laser hit

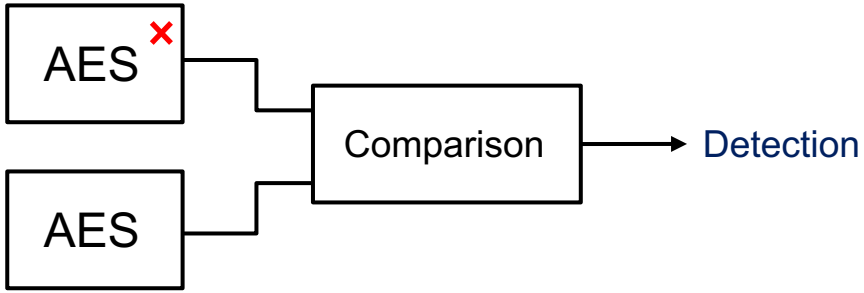
Countermeasures

- Basics – Hardware redundancy



Countermeasures

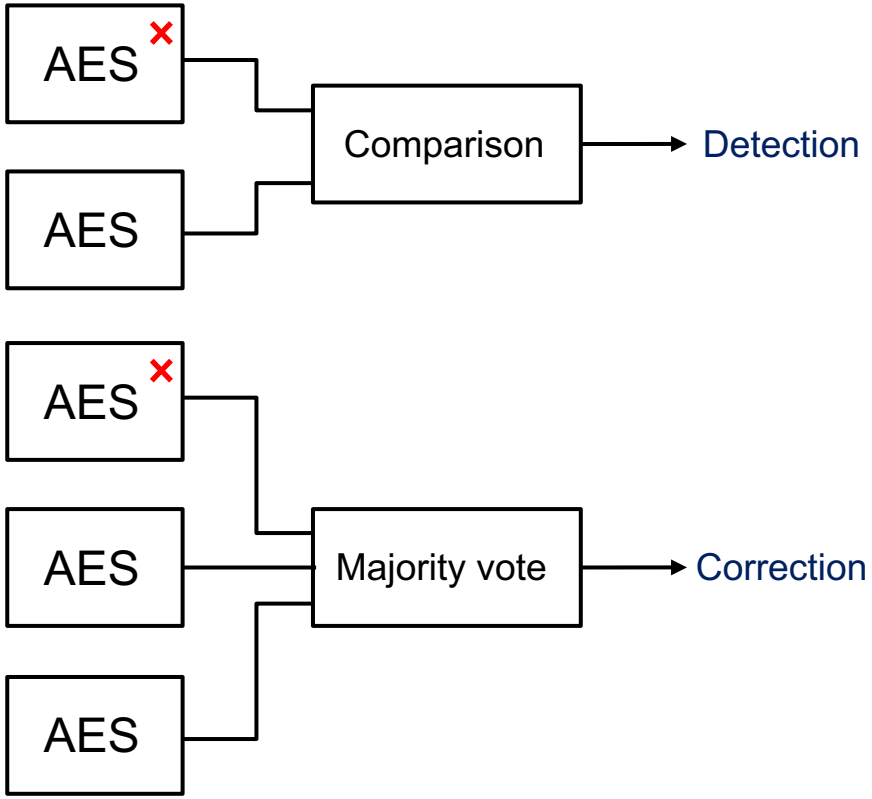
- Basics – Hardware redundancy



✕ Laser hit

Countermeasures

- Basics – Hardware redundancy

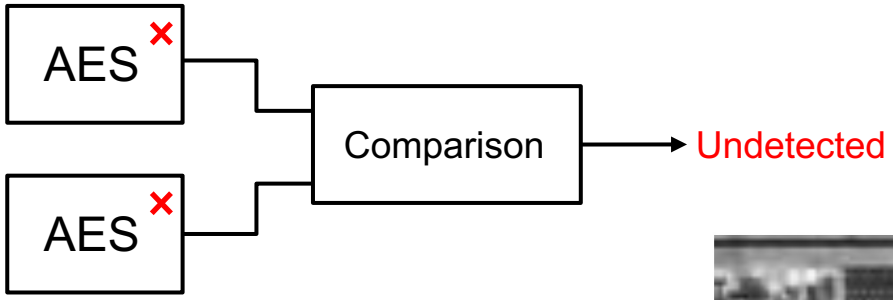


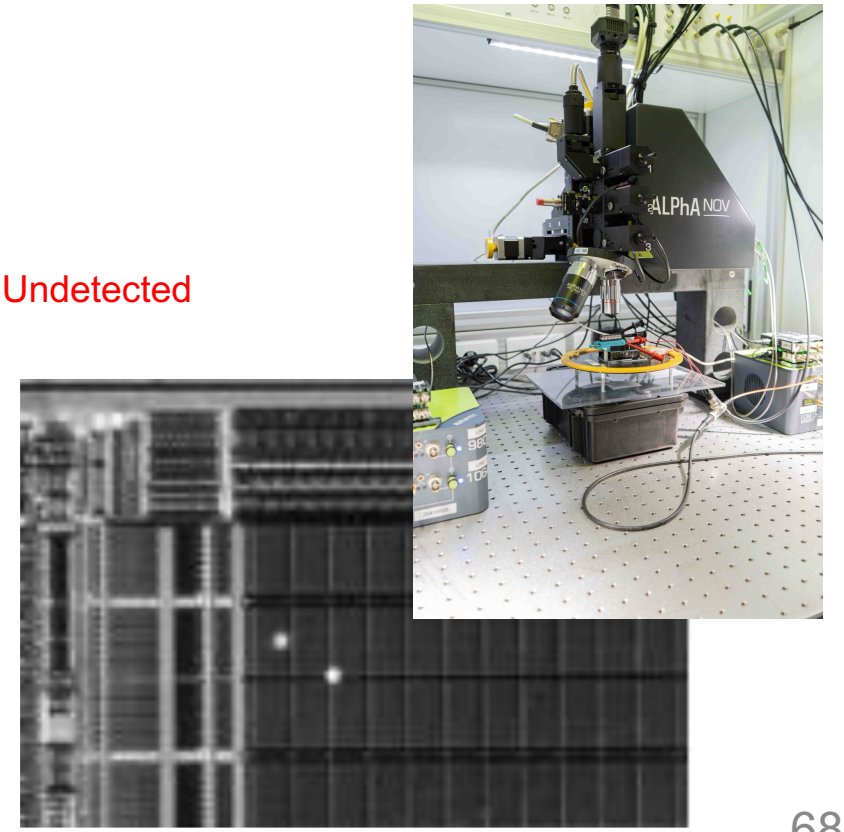
✕ Laser hit

Countermeasures

- Basics – Hardware redundancy

→ Multi-spots laser!





Multi-spot laser fault injection setup : New possibilities for fault injection attacks, B. Colombier et al., Cardis 2022