SEU sensitivity and modeling using picosecond pulsed laser stimulation of a D Flip-Flop in 40 nm CMOS technology

Clément Champeix [1][2], Nicolas Borrel [1][3], Jean-Max Dutertre [2], Bruno Robisson [4], Mathieu Lisart [1] and Alexandre Sarafianos [1]

(1) **STMicroelectronics**
Secure Microcontrollers Division (SMD), 13106 Rousset France

(2) **École Nationale Supérieure des Mines de Saint-Etienne**
Laboratoire Secure Architectures and Systems (LSAS)
Centre de Microélectronique de Provence, 13541 Gardanne, France

(3) **Aix Marseille Université**
CNRS, Université de Toulon, IM2NP UMR 7334, 13397, Marseille, France

(4) **CEA Cadarache**
13108, Saint-Paul-lez-Durance, France

28th IEEE Defect and Fault Tolerance in VLSI and Nanotechnology Systems Symposium

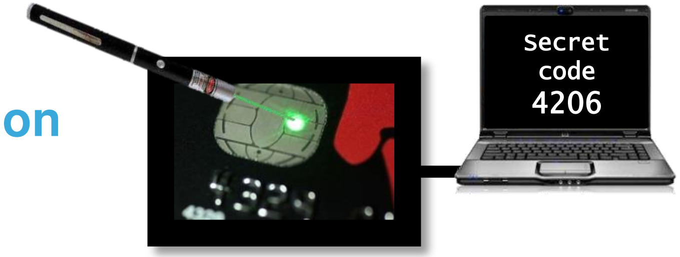
University of Massachusetts Amherst
Tuesday October 13, 2015

Introduction and state of the art

Introduction

- Laser fault injection may be used to **alter the behavior** of an integrated circuit (IC)
  - e.g. **retrieve/modify** secret data in integrated circuit

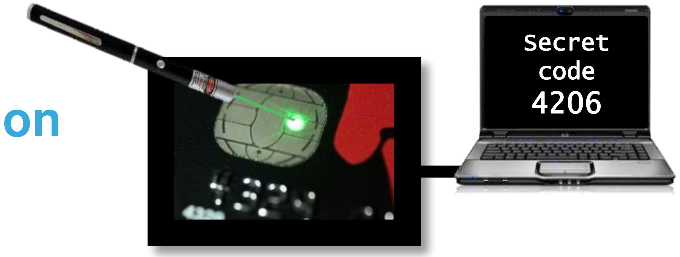
Laser fault injection



Introduction

- Laser fault injection may be used to **alter the behavior** of an integrated circuit (IC)
  - e.g. **retrieve/modify** secret data in integrated circuit

Laser fault injection

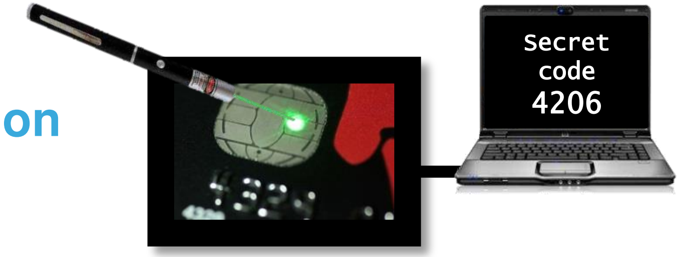


- Sensors are used to **catch** and **flag** when a perturbation is induced

Introduction

- Laser fault injection may be used to **alter the behavior** of an integrated circuit (IC)
  - e.g. **retrieve/modify** secret data in integrated circuit

Laser fault injection



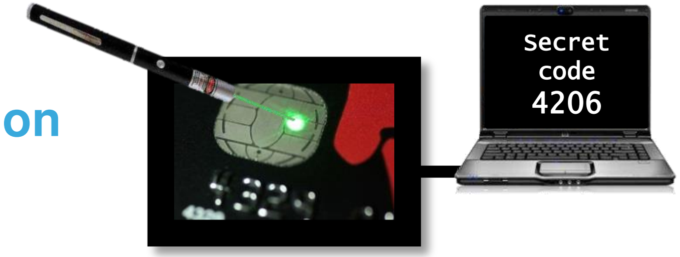
- Sensors are used to **catch** and **flag** when a perturbation is induced

- **Logical gates designs** may be **robust** to laser injection

Introduction

- Laser fault injection may be used to **alter the behavior** of an integrated circuit (IC)
  - e.g. **retrieve/modify** secret data in integrated circuit

Laser fault injection



- Sensors are used to **catch** and **flag** when a perturbation is induced

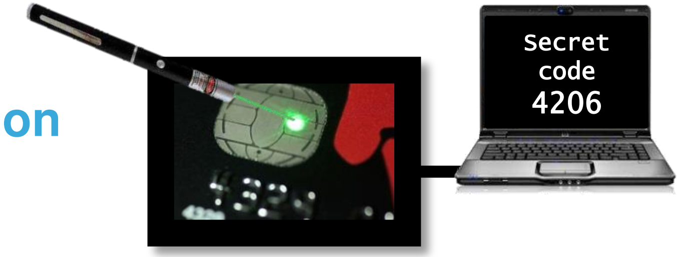
- **Logical gates designs** may be **robust** to laser injection

- **Models** make it possible to simulate the response of ICs to laser pulses

Introduction

- Laser fault injection may be used to **alter the behavior** of an integrated circuit (IC)
  - e.g. **retrieve/modify** secret data in integrated circuit

Laser fault injection



- Sensors are used to **catch** and **flag** when a perturbation is induced

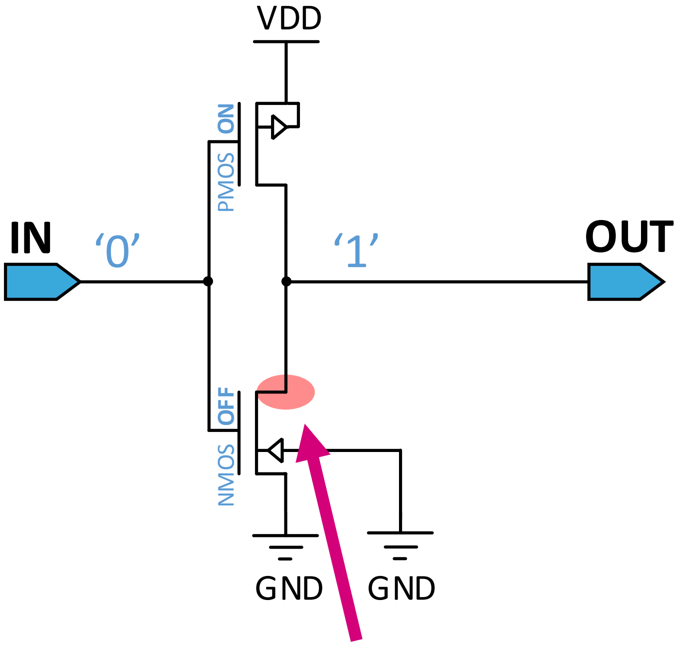
- **Logical gates designs** may be **robust** to laser injection

- **Models** make it possible to simulate the response of ICs to laser pulses

- This presentation reports the experimental analyze of a **D Flip-Flop cell**, designed in **CMOS 40 nm**, under Photoelectric Laser Stimulation (**PLS**) and the **upgrade of electrical laser models**

Single-Events Effects (SEE)

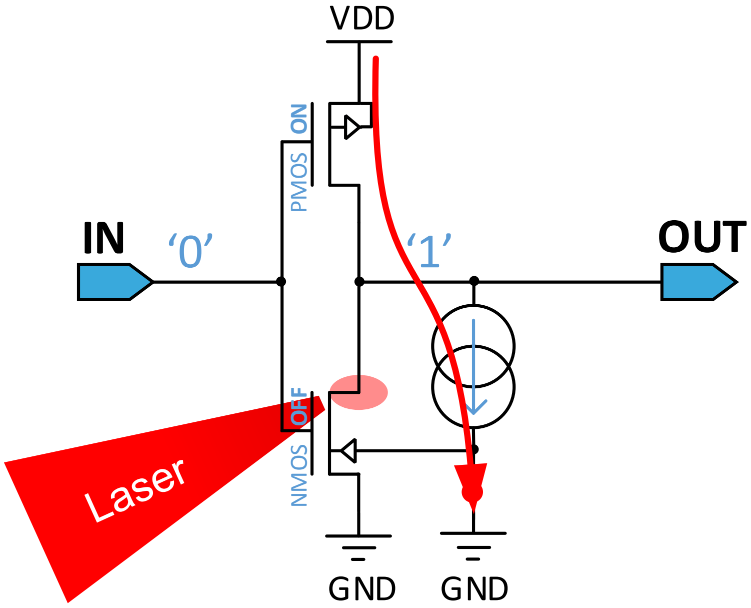
- Example: Laser effect on a **CMOS inverter** with its input at low level
  - Sensitive junction is the **Drain** of NMOS which is in OFF state



Sensitive junction

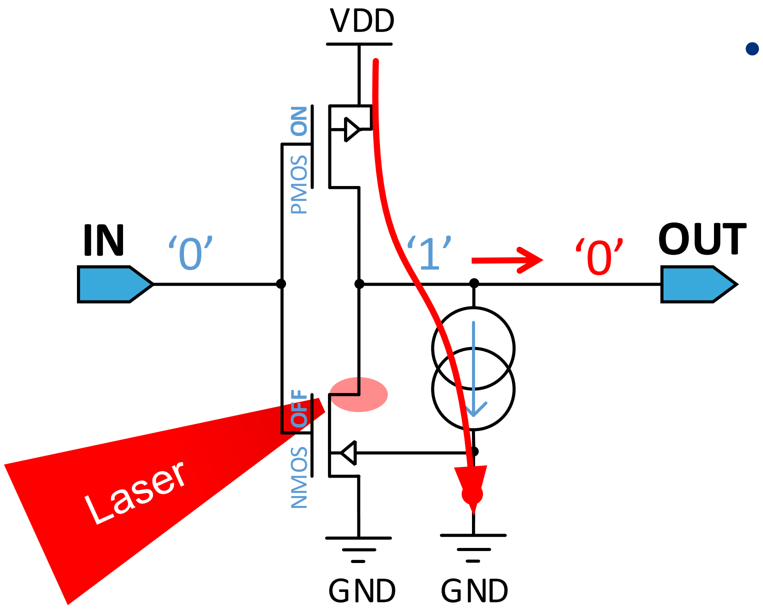
Single-Events Effects (SEE)

- Example: Laser effect on a **CMOS inverter** with its input at low level
  - Sensitive junction is the **Drain** of NMOS which is in OFF state
  - Photocurrent flows **through the Psubstrate**



Single-Events Effects (SEE)

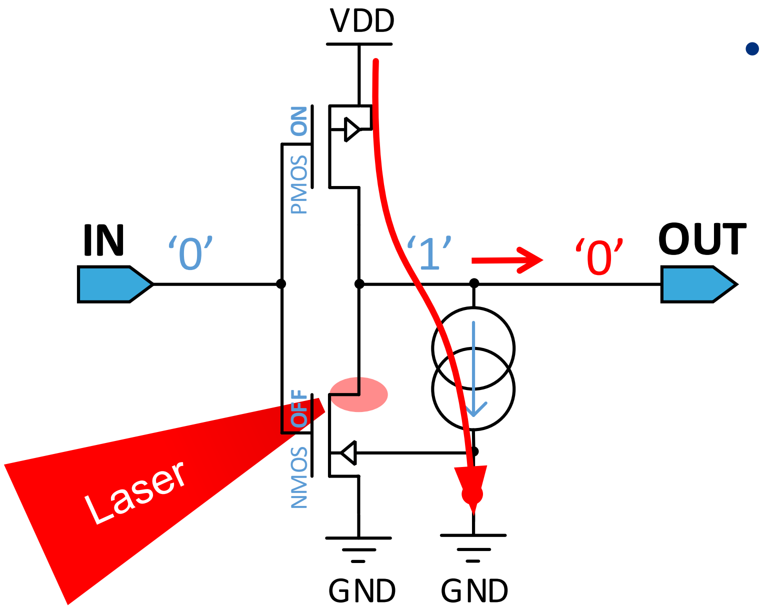
- Example: Laser effect on a **CMOS inverter** with its input at low level
  - Sensitive junction is the **Drain** of NMOS which is in OFF state
  - Photocurrent flows **through the Psubstrate**



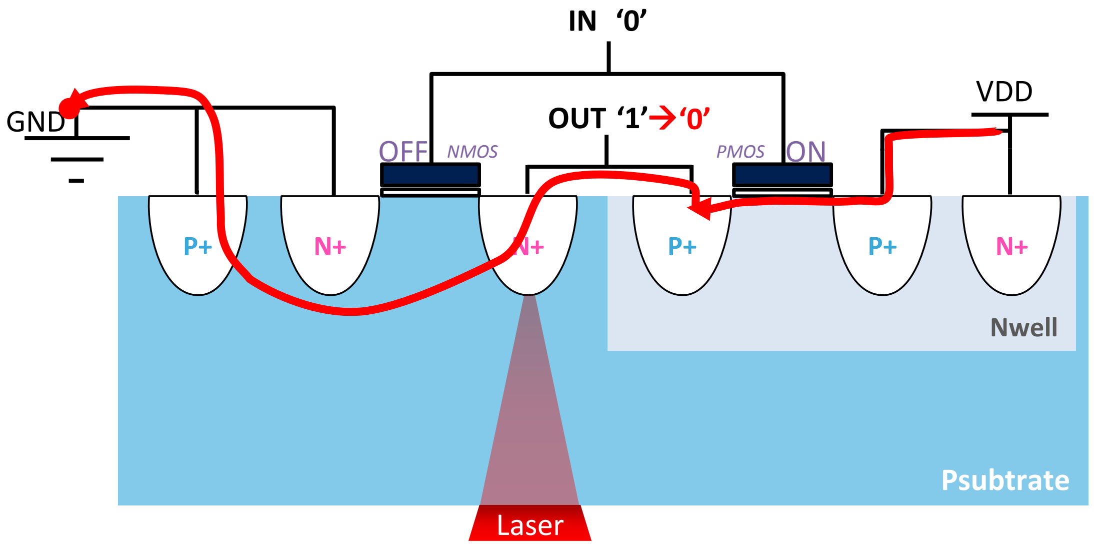
- State of the output **from '1' to '0'**

Single-Events Effects (SEE)

- Example: Laser effect on a **CMOS inverter** with its input at low level
  - Sensitive junction is the **Drain** of NMOS which is in OFF state
  - Photocurrent flows **through the Psubstrate**



- State of the output **from '1' to '0'**



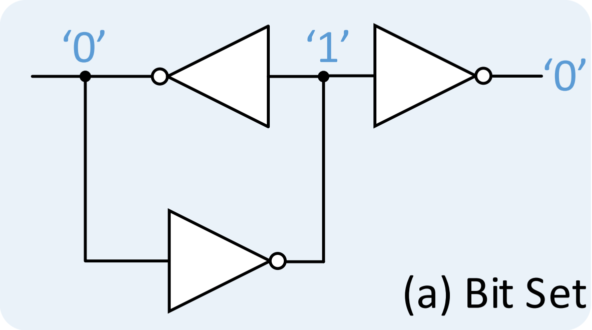
Single-Events Effects (SEE)

- Example: Laser effect on a **Latch**
  - **Single-Events Upset** (SEU) for Bit Set and Bit Reset

Single-Events Effects (SEE)

- Example: Laser effect on a **Latch**
  - **Single-Events Upset** (SEU) for Bit Set and Bit Reset

- **Bit Set**

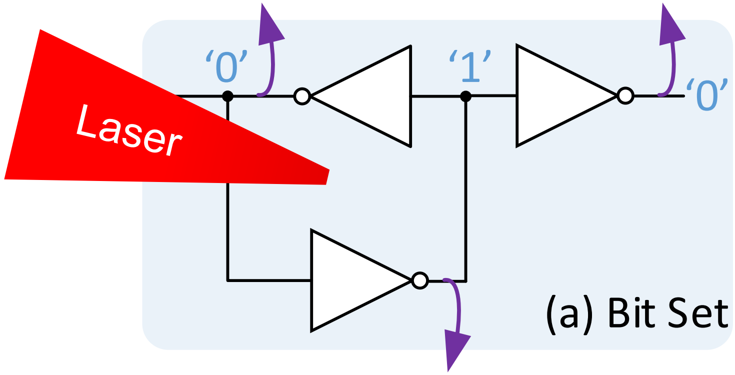


(a) Bit Set

Single-Events Effects (SEE)

- Example: Laser effect on a **Latch**
  - **Single-Events Upset** (SEU) for Bit Set and Bit Reset

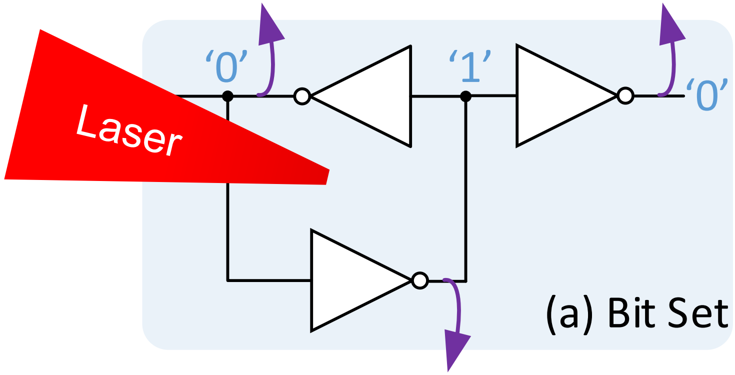
- **Bit Set**

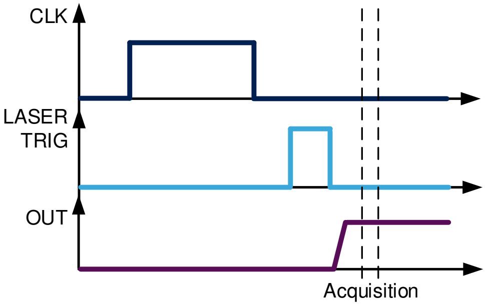


Single-Events Effects (SEE)

- Example: Laser effect on a **Latch**
  - **Single-Events Upset** (SEU) for Bit Set and Bit Reset

- **Bit Set**
  - State of the output **from ‘0’ to ‘1’**

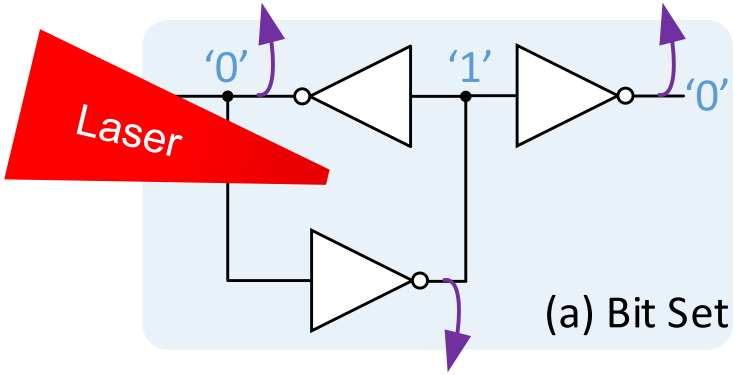


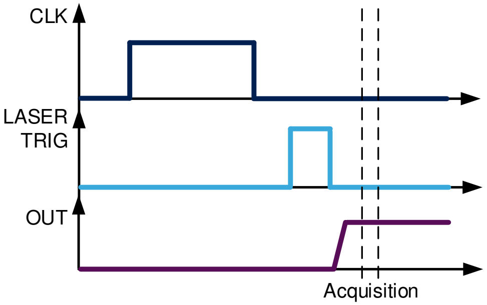


Single-Events Effects (SEE)

- Example: Laser effect on a **Latch**
  - **Single-Events Upset** (SEU) for Bit Set and Bit Reset

- **Bit Set**
  - State of the output **from ‘0’ to ‘1’**

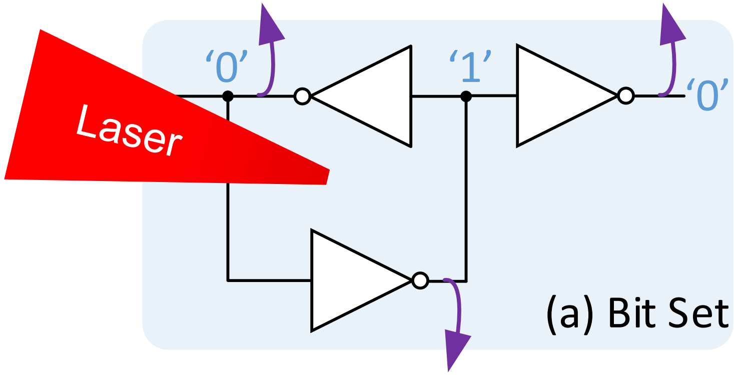


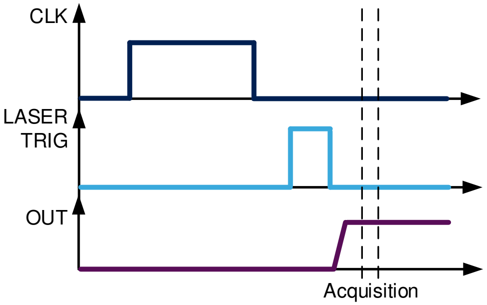


Single-Events Effects (SEE)

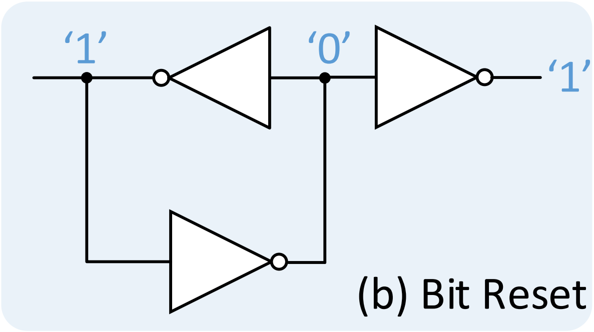
- Example: Laser effect on a **Latch**
  - **Single-Events Upset** (SEU) for Bit Set and Bit Reset

- **Bit Set**
  - State of the output **from '0' to '1'**





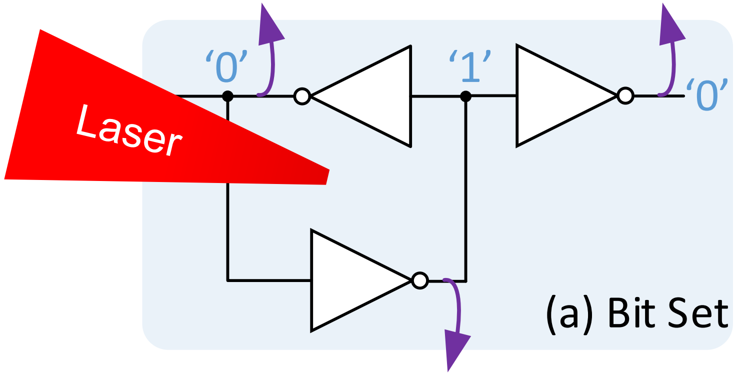
- **Bit Reset**

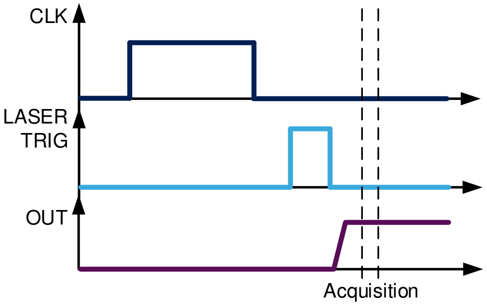


Single-Events Effects (SEE)

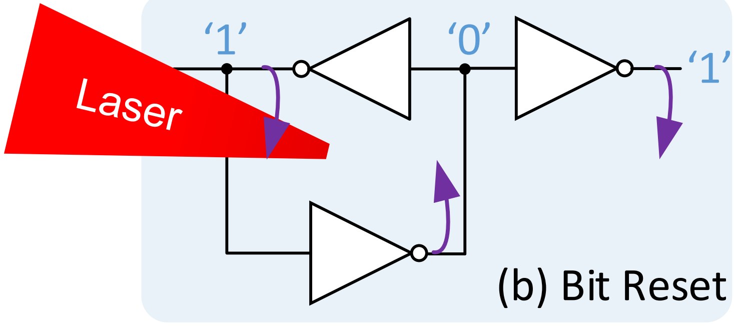
- Example: Laser effect on a **Latch**
  - **Single-Events Upset** (SEU) for Bit Set and Bit Reset

- **Bit Set**
  - State of the output **from ‘0’ to ‘1’**





- **Bit Reset**

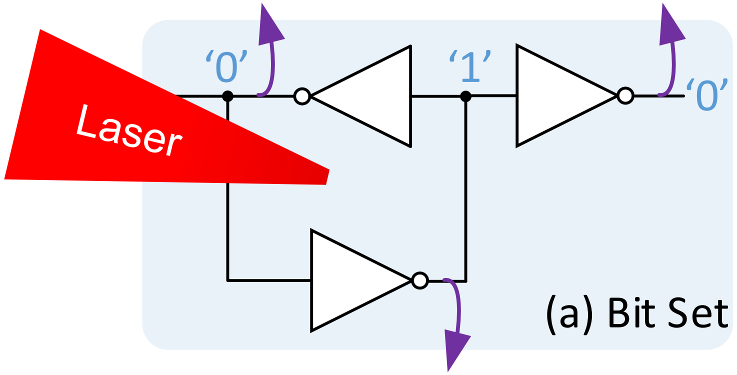


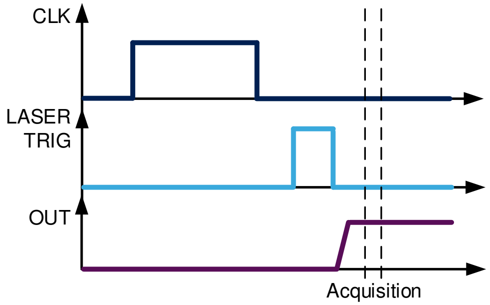
Single-Events Effects (SEE)

- Example: Laser effect on a **Latch**
  - **Single-Events Upset** (SEU) for Bit Set and Bit Reset

Bit Set

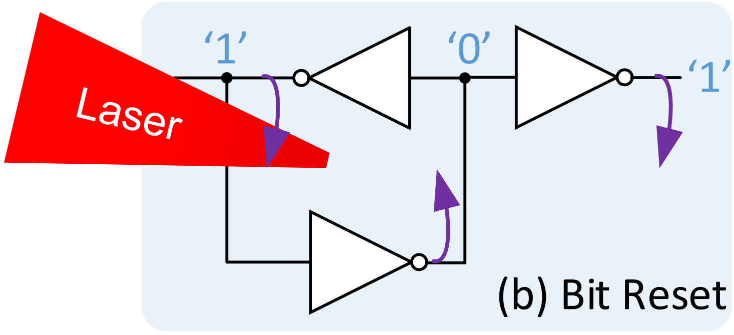
- State of the output **from '0' to '1'**

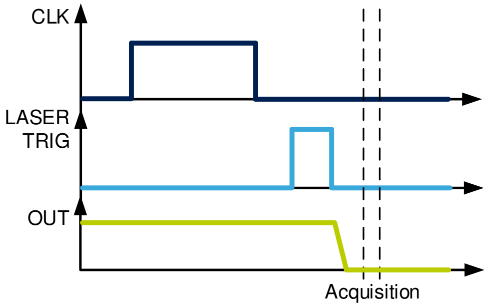




Bit Reset

- State of the output **from '1' to '0'**





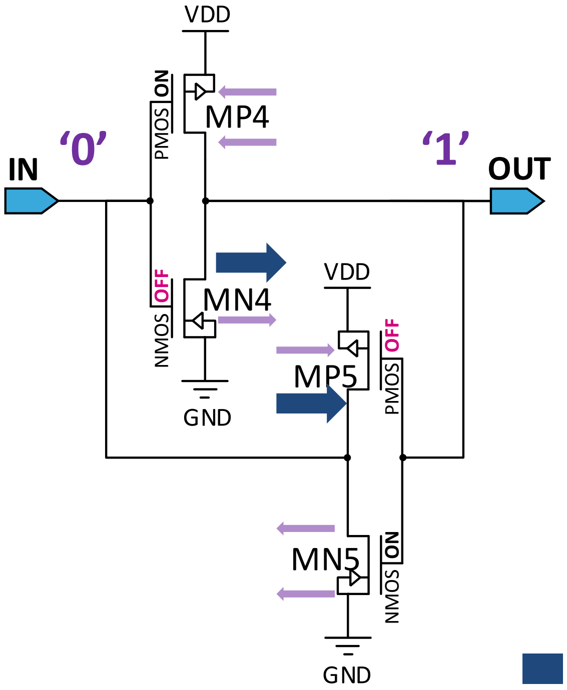
Latch sensitivity

- Schematic of a latch cell **laser sensitivity area** with input at ‘0’ and ‘1’

Latch sensitivity

- Schematic of a latch cell **laser sensitivity area** with input at ‘0’ and ‘1’
  - The purple arrows give the **photocurrent directions** and its **strength**

(a) Input at ‘0’

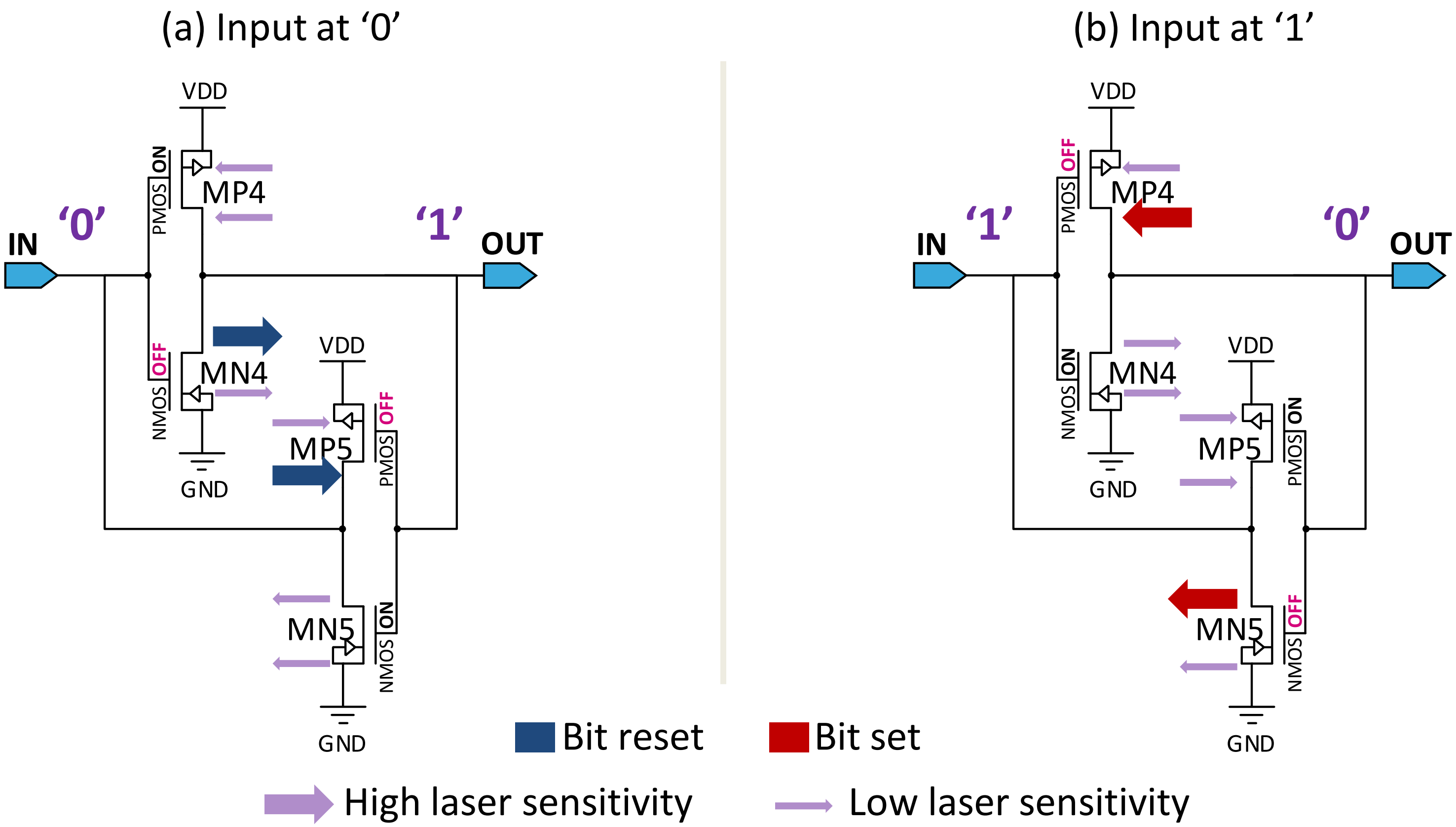


🟦 Bit reset 🟥 Bit set

High laser sensitivity → Low laser sensitivity

Latch sensitivity

- Schematic of a latch cell **laser sensitivity area** with input at ‘0’ and ‘1’
  - The purple arrows give the **photocurrent directions** and its **strength**

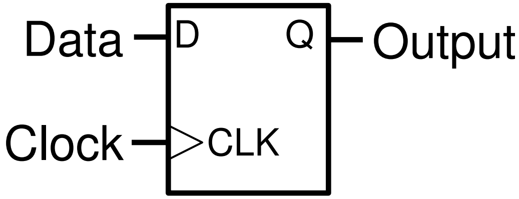


(a) Input at ‘0’

(b) Input at ‘1’

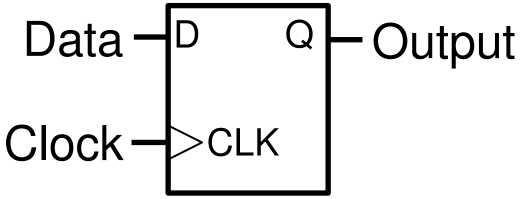
D Flip Flop description

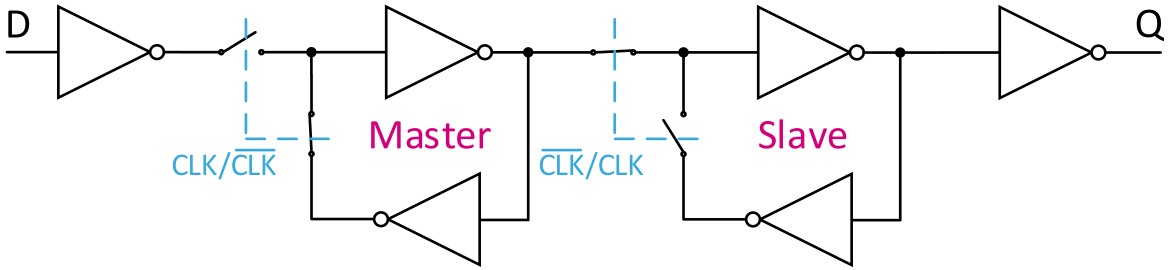
- A D Flip-Flop is a memorizing cell
  - **Store information** and many **other uses**
  - **More than a thousand** in an integrated circuit
    - It becomes mandatory to **thwart laser attacks** (weakness point)



D Flip Flop description

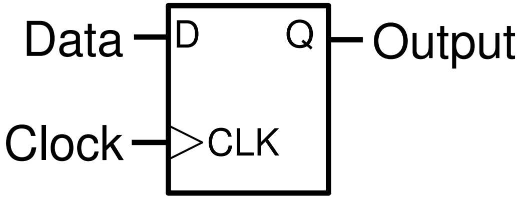
- A D Flip-Flop is a memorizing cell
  - **Store information** and many **other uses**
  - **More than a thousand** in an integrated circuit
    - It becomes mandatory to **thwart laser attacks** (weakness point)

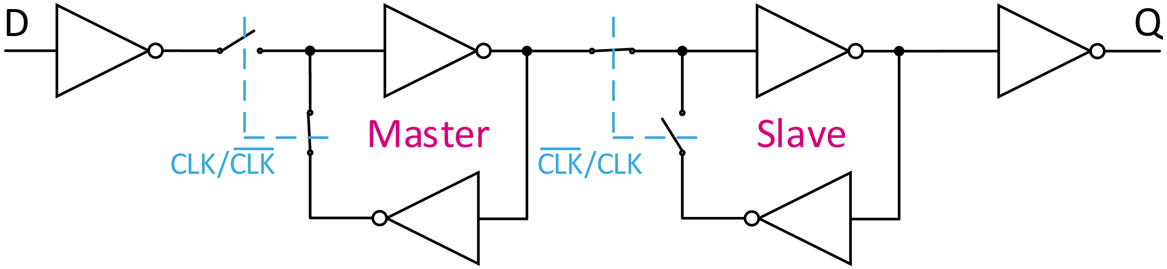




D Flip Flop description

- A D Flip-Flop is a memorizing cell
  - **Store information** and many **other uses**
  - **More than a thousand** in an integrated circuit
    - It becomes mandatory to **thwart laser attacks** (weakness point)





CLK	D	Q_{next}	Comments
Rising Edge	0	0	$Q_{next} = D = 0$
Rising Edge	1	1	$Q_{next} = D = 1$
Non Rising	X	Q	Memorizing

- D Flip-Flop functioning
  - **Change** state at rising edge
  - **Memorize** during non rising

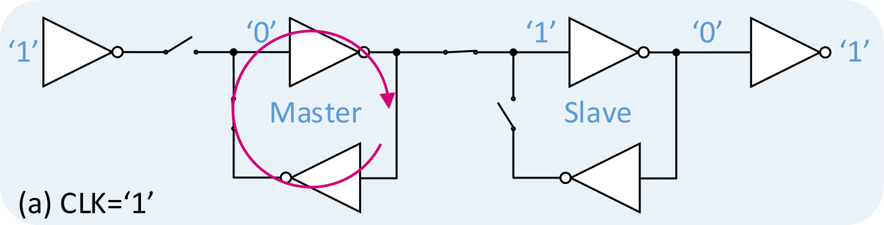
D Flip Flop evaluations

- 4 steps to impact **master** or **slave** latch

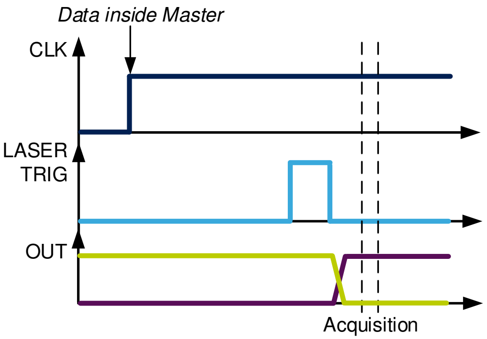
D Flip Flop evaluations

- 4 steps to impact **master** or **slave** latch

- **CLK = ‘1’**



(a) CLK=‘1’

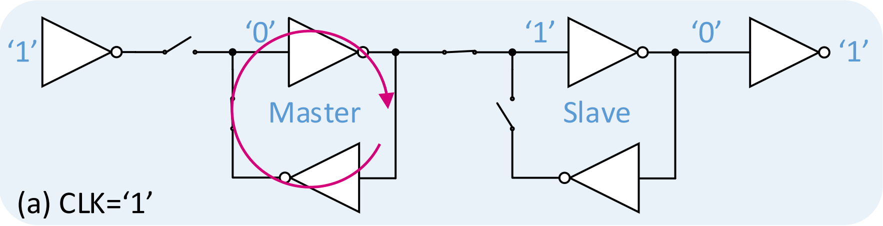


(b) CLK=‘1’

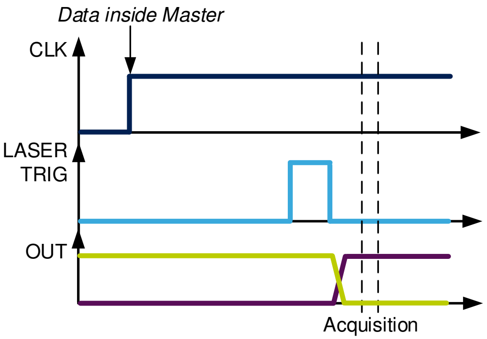
D Flip Flop evaluations

- 4 steps to impact **master** or **slave** latch

- **CLK = ‘1’**

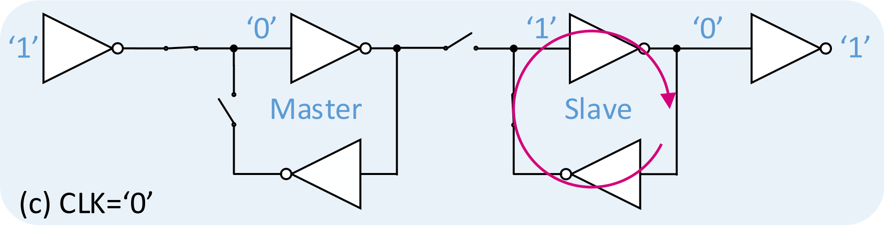


(a) CLK=‘1’

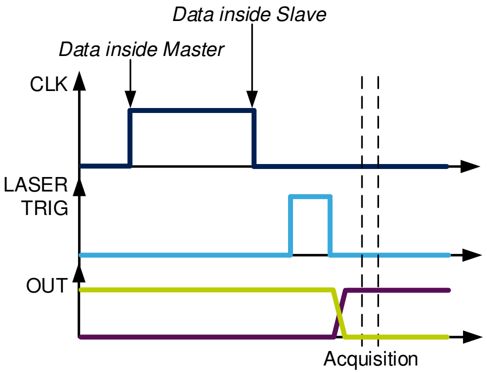


(b) CLK=‘1’

- **CLK = ‘0’**



(c) CLK=‘0’

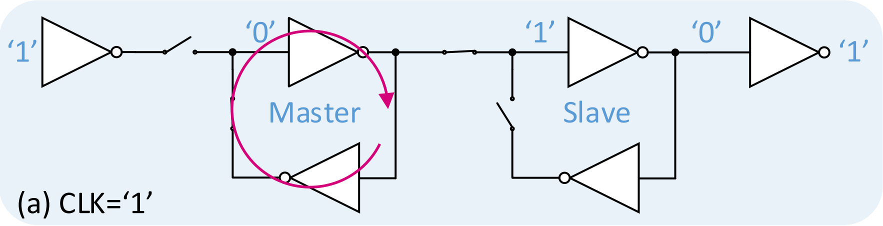


(d) CLK=‘0’

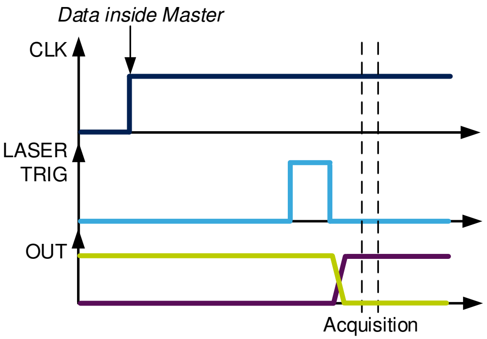
D Flip Flop evaluations

- 4 steps to impact **master** or **slave** latch

- **CLK = ‘1’**

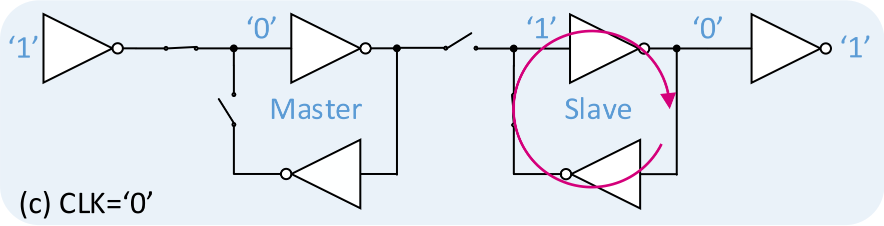


(a) CLK=‘1’

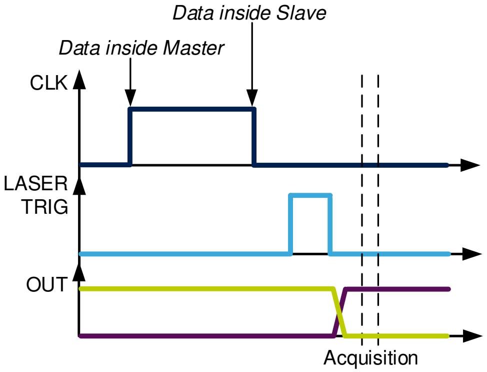


(b) CLK=‘1’

- **CLK = ‘0’**



(c) CLK=‘0’



(d) CLK=‘0’

- 4 steps →

Steps number	Input (D)	Clock (CLK)	Comments
Step 1	0	0	Bit set / Slave impacted
Step 2	0	1	Bit set / Master impacted
Step 3	1	0	Bit reset / Slave impacted
Step 4	1	1	Bit reset / Master impacted

Device Under Test (DUT)

D Flip-Flop schematic

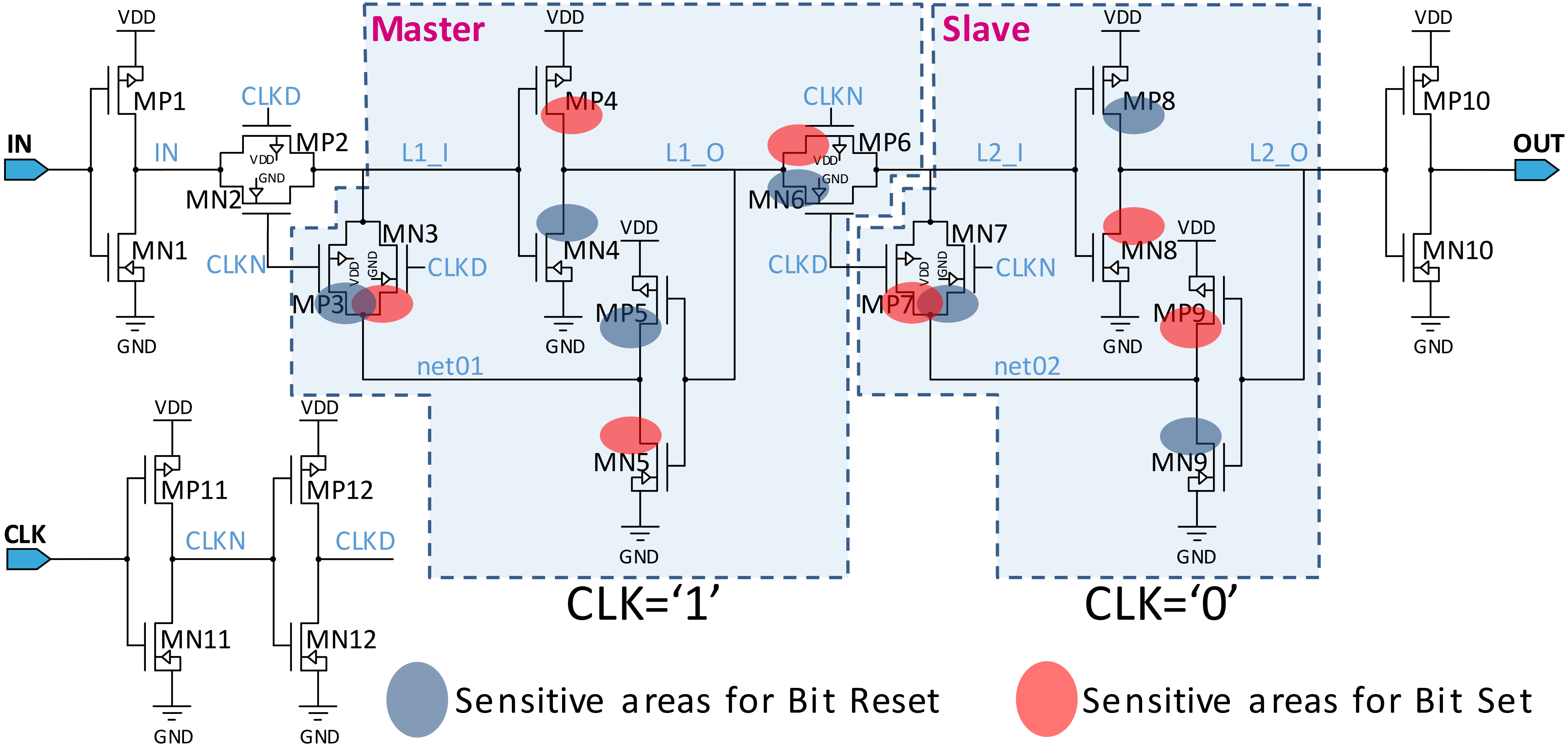
- Theoretical hypothesis
  - Sensitive areas on **schematic**

- 40 nm CMOS technology

D Flip-Flop schematic

- Theoretical hypothesis
    - Sensitive areas on **schematic**

- 40 nm CMOS technology



● Sensitive areas for Bit Reset

● Sensitive areas for Bit Set

D Flip-Flop layout

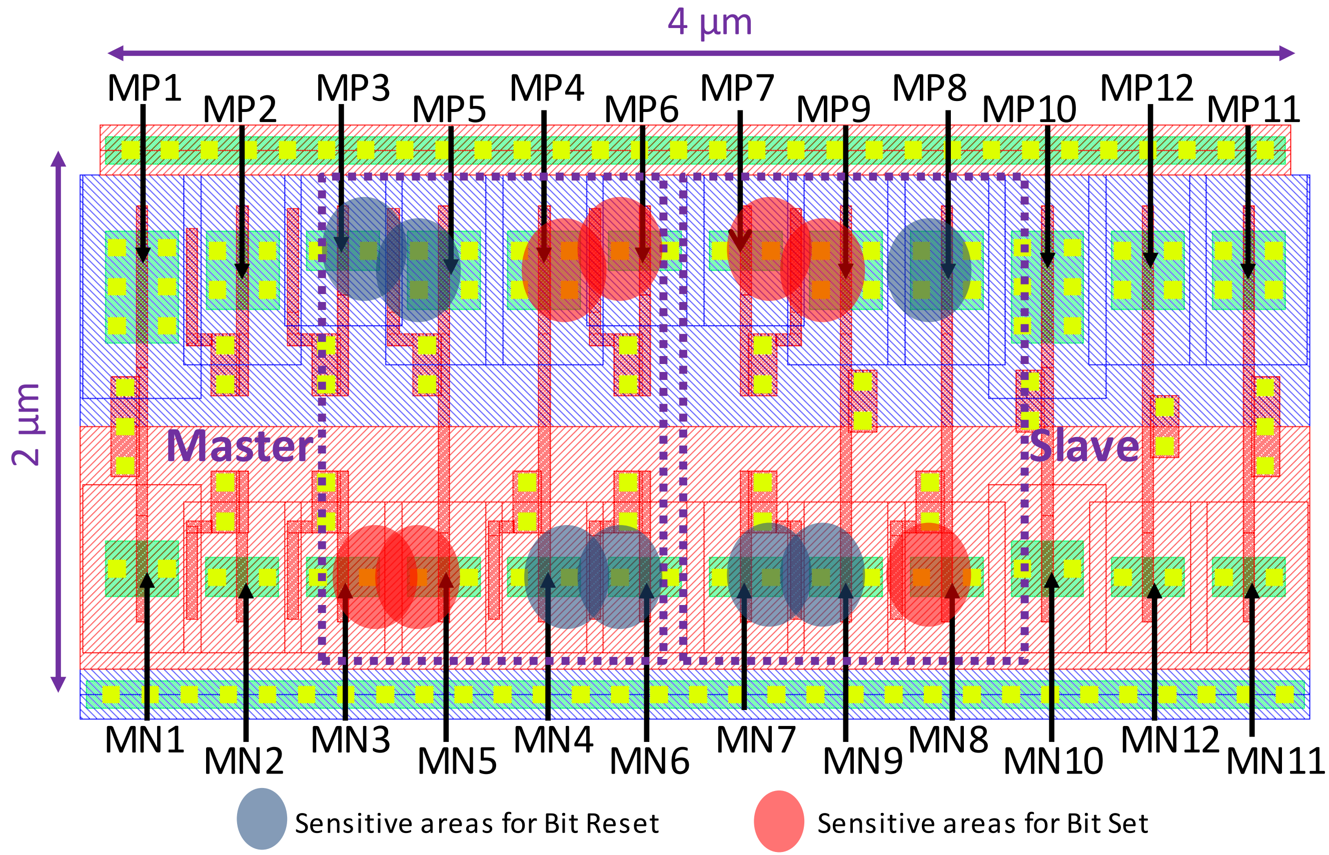
- 40 nm CMOS technology

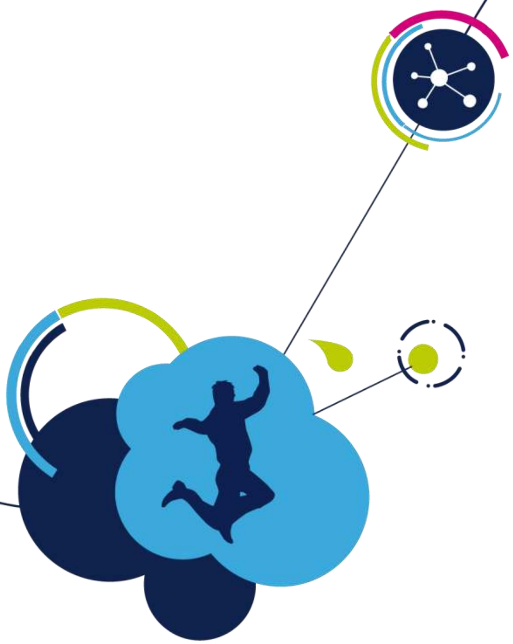
- Theoretical hypothesis
  - Sensitive areas on corresponding **layout**

D Flip-Flop layout

- 40 nm CMOS technology

- Theoretical hypothesis
  - Sensitive areas on corresponding **layout**

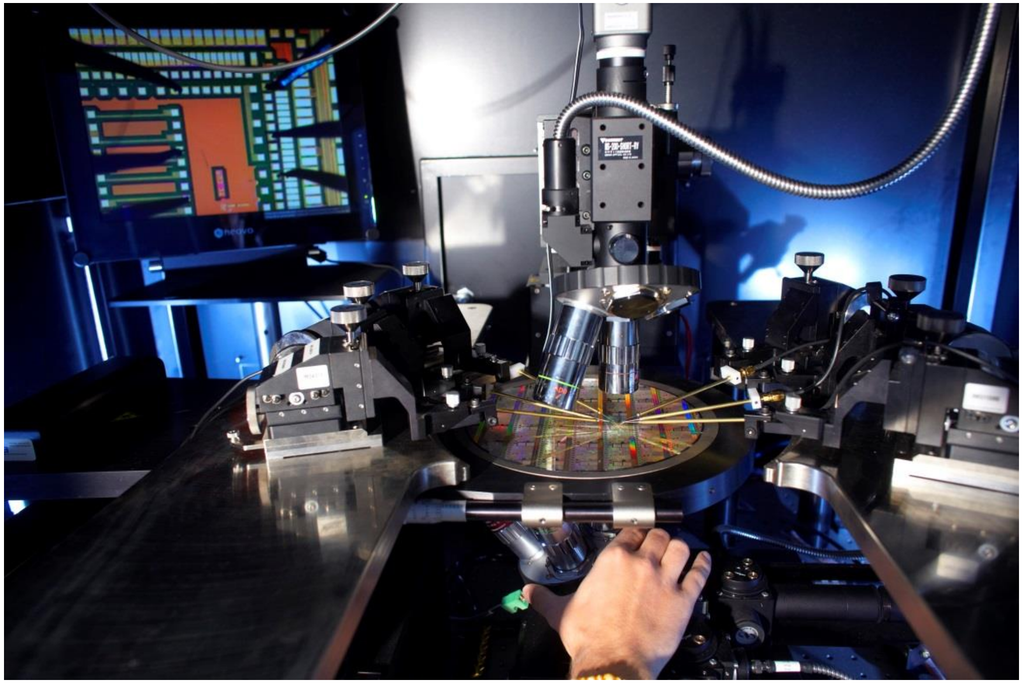




Experiments

Experiments settings

- Experimental set up
  - Wavelength: **1030 nm** (near Infra Red)
  - Spot size: **~ 1 µm** (100X lens)
  - Laser through silicon substrate **backside**
  - Laser power: **0.7 nJ**
  - Laser pulse duration: **30 ps**
  - Cartography step: **0.2 µm**



Experiments results

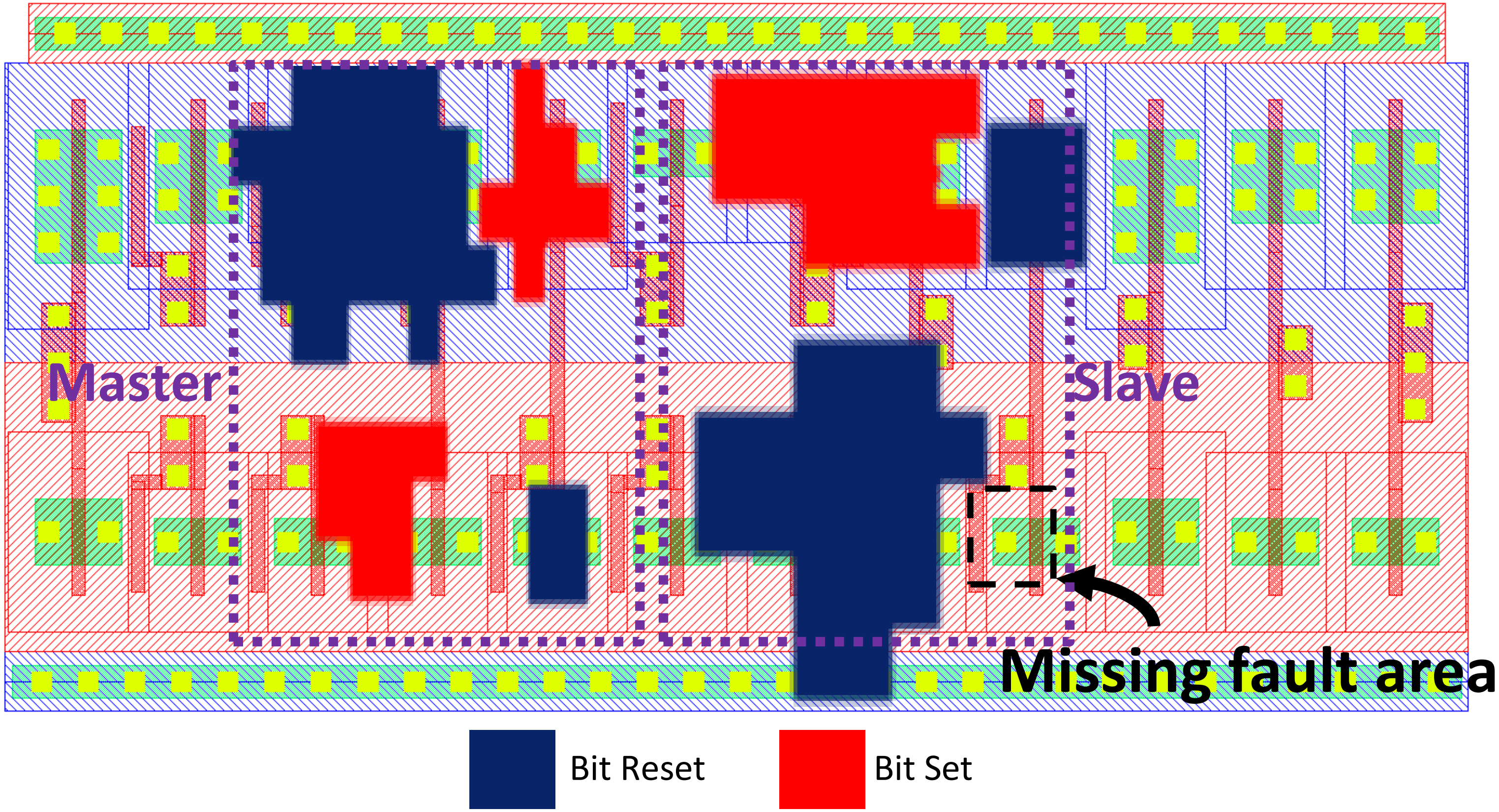
- 40 nm CMOS technology

- Experimental results

Experiments results

- 40 nm CMOS technology

- Experimental results

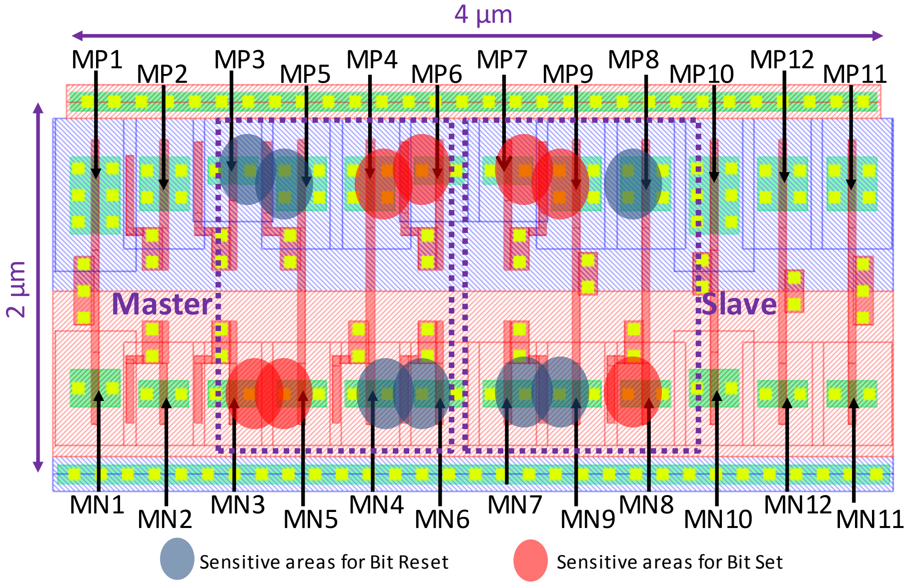


Experiments results

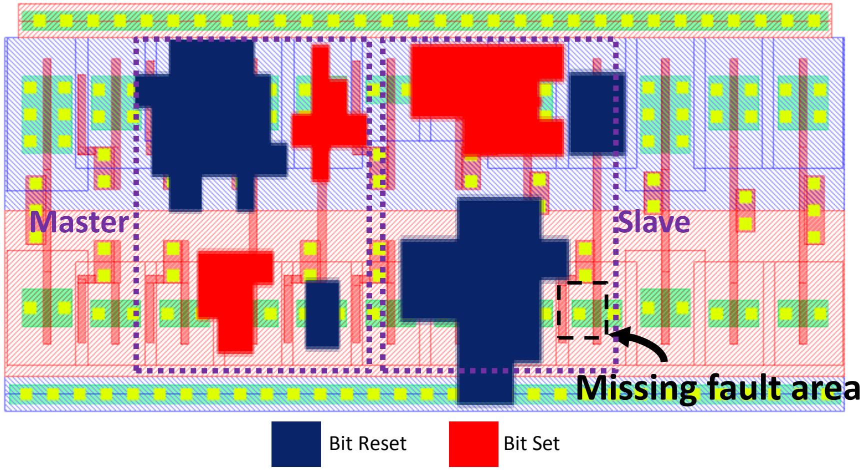
- 40 nm CMOS technology

- Experimental results

  - Basically fit with **theoretical hypothesis**
    - **One missing fault area** because of the capacitor and resistivity of the net



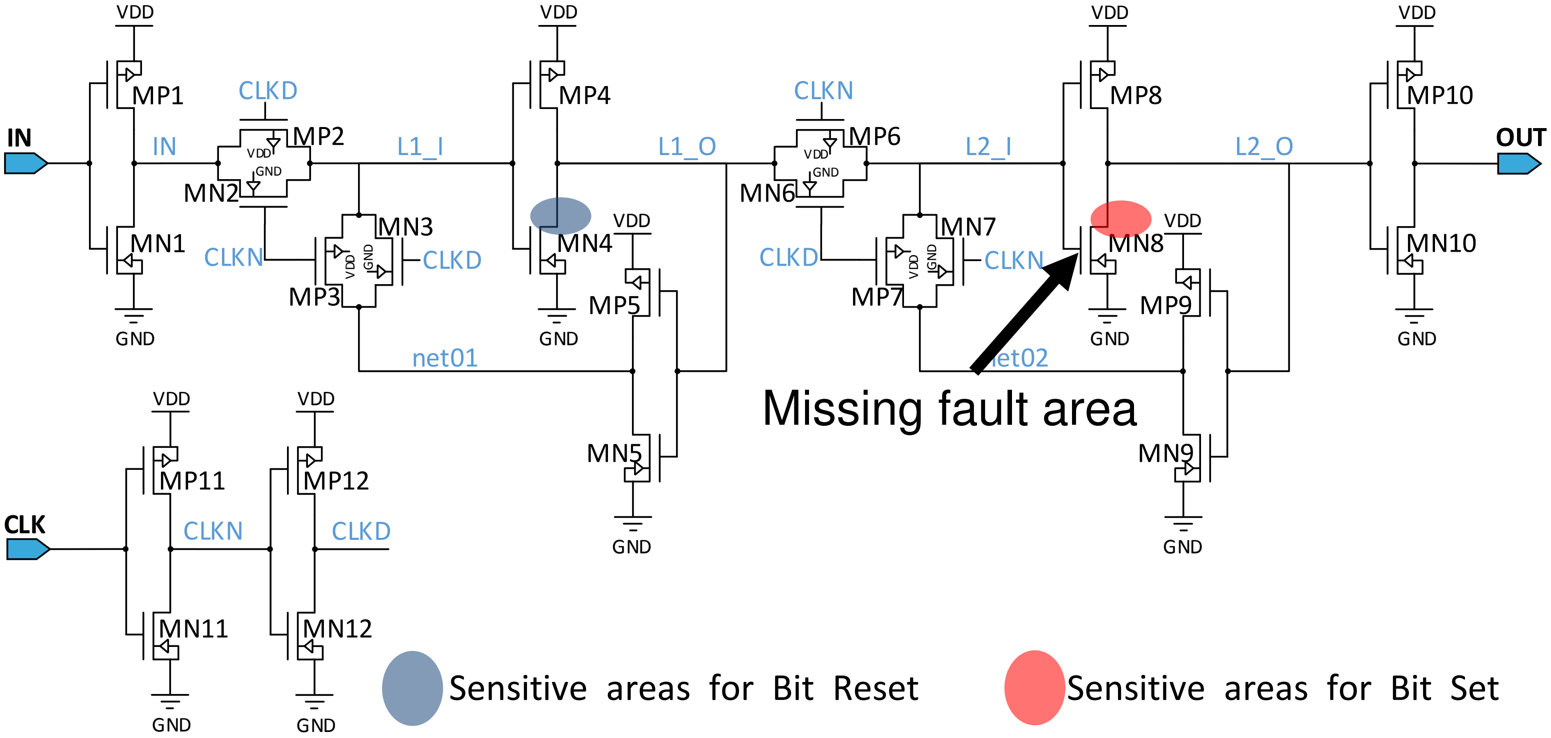
(a) Theoretical hypothesis



(b) Experimental

D Flip-Flop schematic

- 40 nm CMOS technology



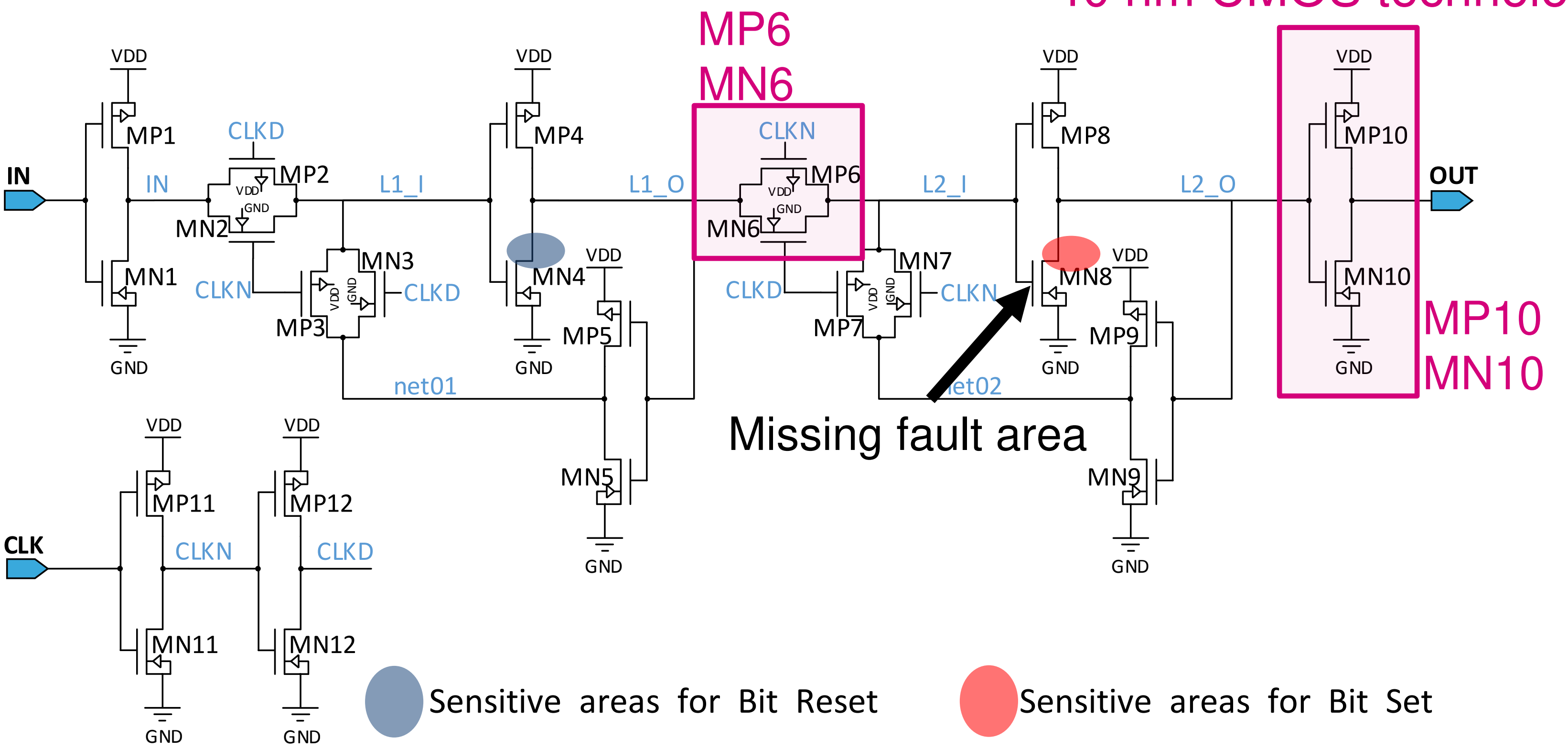
Missing fault area

● Sensitive areas for Bit Reset

● Sensitive areas for Bit Set

D Flip-Flop schematic

- 40 nm CMOS technology



MP6
MN6

MP10
MN10

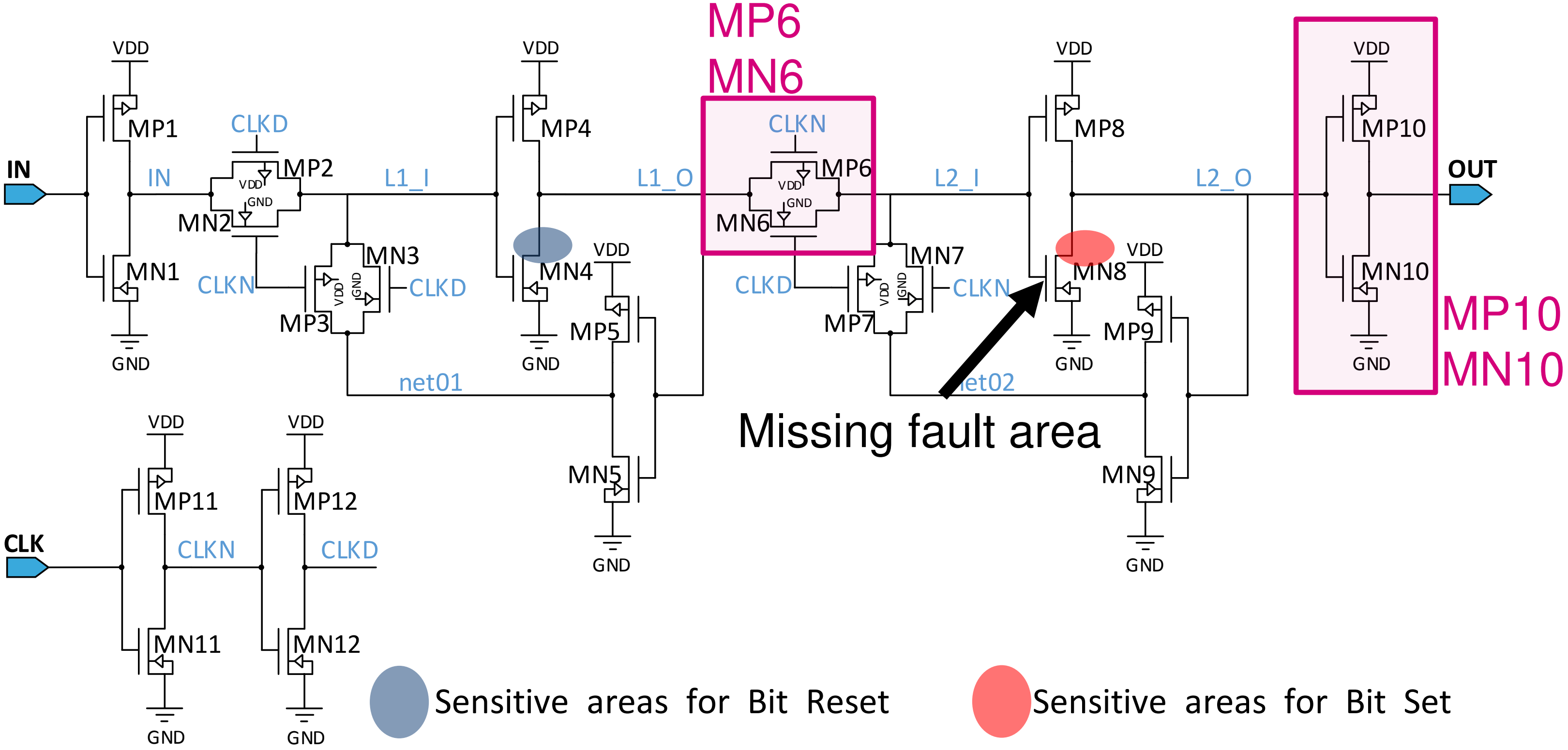
Missing fault area

● Sensitive areas for Bit Reset

● Sensitive areas for Bit Set

D Flip-Flop schematic

- 40 nm CMOS technology



Transistors	Ratio W/L	Comments
MN1, MN10	5	NMOS BUF/INV
MN2, MN3, MN6, MN7	3.5	NMOS Pass gates
MN4, MN5, MN8 MN9, MN11, MN12	3.5	NMOS INV
MP1, MP10	10	PMOS BUF/INV
MP2, MP3, MP6, MP7	3.5	PMOS Pass gates
MP4, MP5, MP8 MP9, MP11, MP12	7	PMOS INV

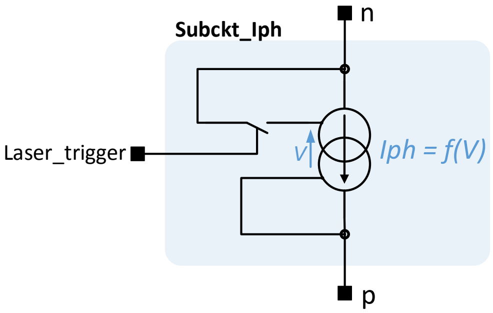
MN10 and MP10 **>** MN6 and MP6

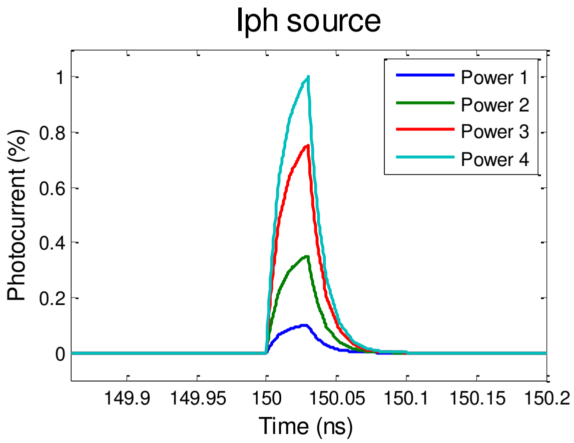
L2_O cap/res **>** L1_O cap/res

Modeling

Modeling settings

- Electrical modeling (*Photoelectrical laser stimulation model*)
  - **Coefficient adjustment** for picosecond laser pulse duration



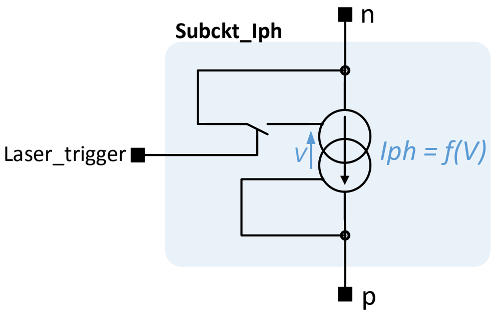


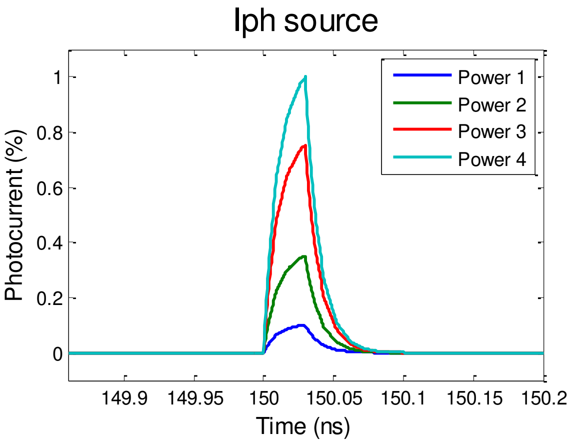
$$\boxed{I_{ph} = \frac{1}{\gamma}(aV + b)\alpha_{gauss} Pulse_{width} W_{coef} I_{ph\_z}}$$

References: Equations model and applications courtesy ***Alexandre Sarafianos's publications***

Modeling settings

- Electrical modeling (*Photoelectrical laser stimulation model*)
  - **Coefficient adjustment** for picosecond laser pulse duration





$$\boxed{I_{ph} = \frac{1}{\gamma}(aV + b)\alpha_{gauss}\mathrm{Pulse}_{width} W_{coef} I_{ph\_z}}$$

- **V** is the reverse-biased voltage
- **a and b** depend on laser power
- **γ** is an amplification attenuation coefficient
- α_{gauss} is the sum of two gaussian functions (spatial dependency)
- Pulse_{width} considers laser power duration
- W_{coef} is an exponential function for the wafer thickness
- I_{ph_z} is a curve function considering the focus effect of laser lens

References: Equations model and applications courtesy ***Alexandre Sarafianos's publications***

Modeling results

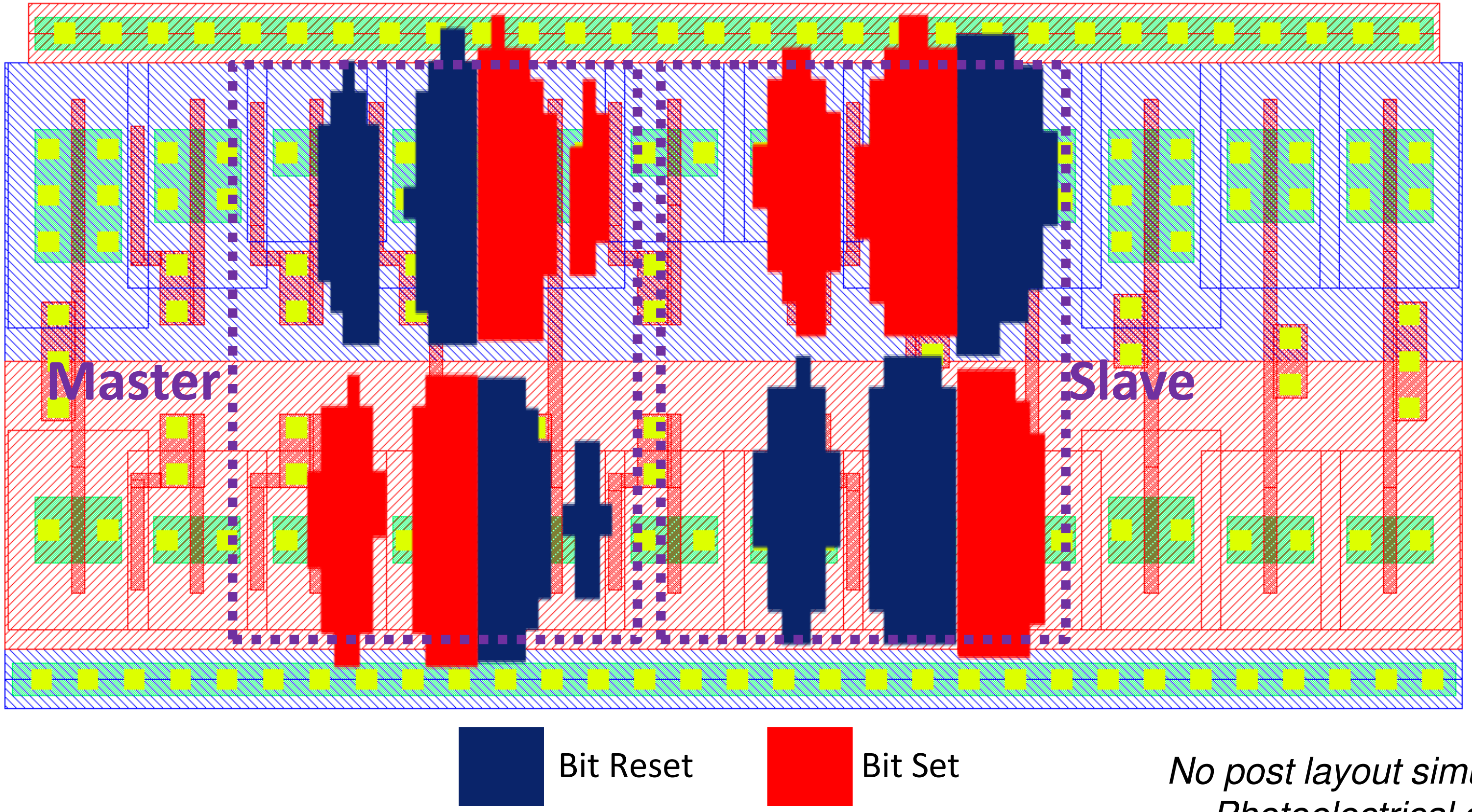
- Modeling results

- 40 nm CMOS technology

Modeling results

- Modeling results

- 40 nm CMOS technology

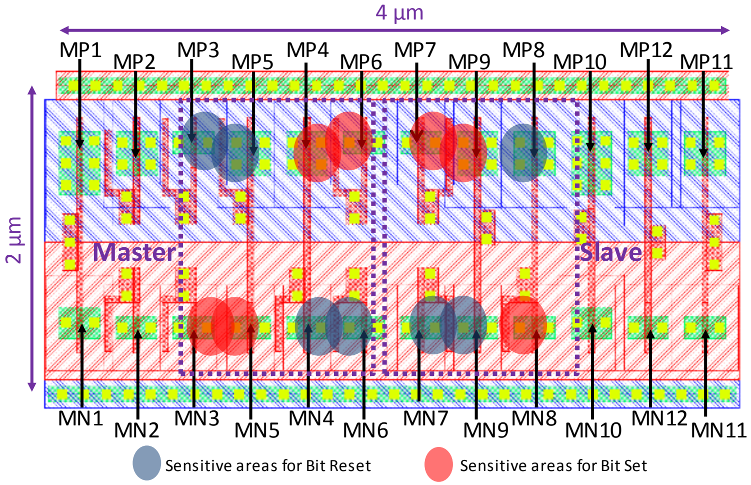


No post layout simulation
Photoelectrical only

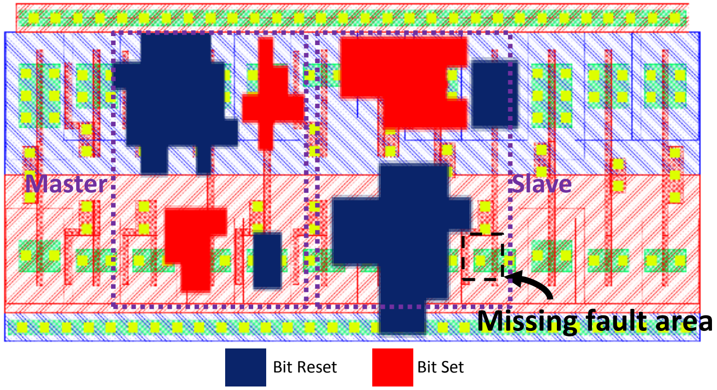
Modeling results

- 40 nm CMOS technology

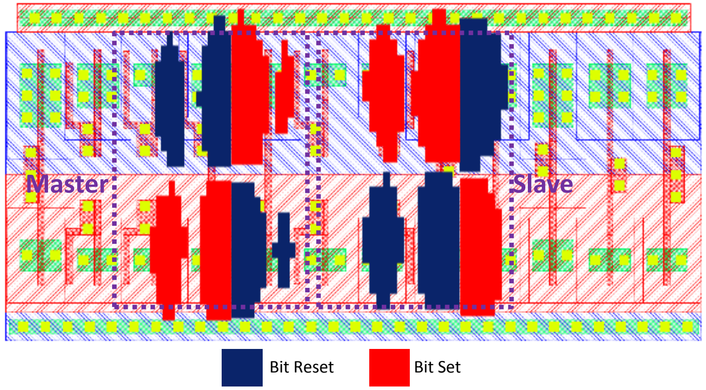
- Modeling results
  - Basically fit with **theoretical hypothesis** and **experimental**



(a) Theoretical hypothesis



(b) Experimental



(c) Modeling

No post layout simulation
Photoelectrical only

Conclusion and perspectives

Conclusion and perspectives

- Conclusion
  - **Analysis of laser fault injection** of a CMOS 40nm D Flip-Flop cell and the **upgrading** of photoelectrical laser stimulation models

Conclusion and perspectives

- Conclusion
  - **Analysis of laser fault injection** of a CMOS 40nm D Flip-Flop cell and the **upgrading** of photoelectrical laser stimulation models
  - **Good correlation** between photoelectrical hypothesis, experiments and models

Conclusion and perspectives

- Conclusion
  - **Analysis of laser fault injection** of a CMOS 40nm D Flip-Flop cell and the **upgrading** of photoelectrical laser stimulation models
  - **Good correlation** between photoelectrical hypothesis, experiments and models

- Perspectives and future works
  - The models will be enhance to take account **capacitors** and **resistivity of the nets**

Conclusion and perspectives

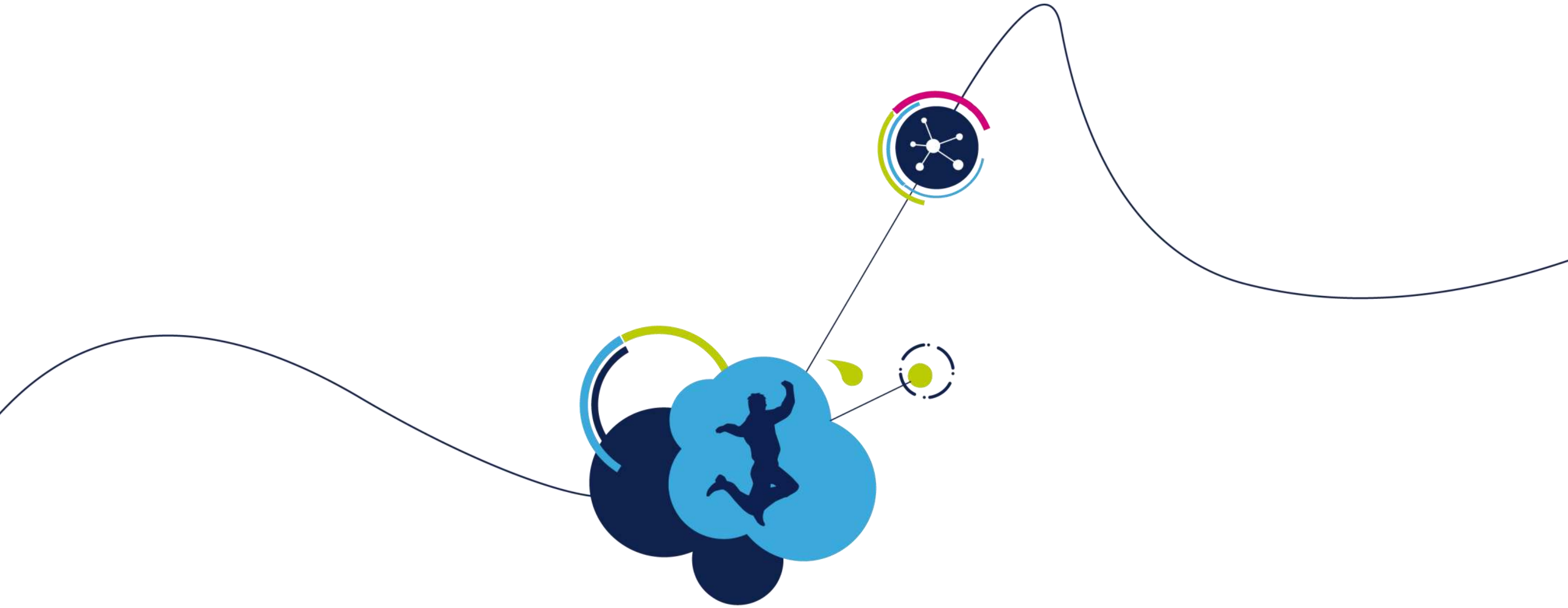
- Conclusion
  - **Analysis of laser fault injection** of a CMOS 40nm D Flip-Flop cell and the **upgrading** of photoelectrical laser stimulation models
  - **Good correlation** between photoelectrical hypothesis, experiments and models

- Perspectives and future works
  - The models will be enhance to take account **capacitors** and **resistivity of the nets**
  - **Flip-flops** will be designed and tested to validate the model and **develop robust cells** to laser fault injection

Conclusion and perspectives

- Conclusion
  - **Analysis of laser fault injection** of a CMOS 40nm D Flip-Flop cell and the **upgrading** of photoelectrical laser stimulation models
  - **Good correlation** between photoelectrical hypothesis, experiments and models

- Perspectives and future works
  - The models will be enhance to take account **capacitors** and **resistivity of the nets**
  - **Flip-flops** will be designed and tested to validate the model and **develop robust cells** to laser fault injection
  - This first step model presented could be an interesting tool for designers who want to **build robust gates** or **test the robustness of our designs**



Thank you for your attention

28th IEEE Defect and Fault Tolerance in VLSI and Nanotechnology Systems Symposium

University of Massachusetts Amherst
Tuesday October 13, 2015

life.augmented MINES Saint-Étienne Im2np cea IEEE defect fault tolerance & in VLSI and nanotechnology systems