ISVLSI 2015
Montpellier

Figure of merits of 28nm Si technologies for implementing laser attack resistant security dedicated circuit

Stéphan de Castro

J-M. Dutertre, G. Di Natale, M.L. Flottes , B. Rouzeyre

Laboratoire Informatique Robotique Microélectronique Montpellier

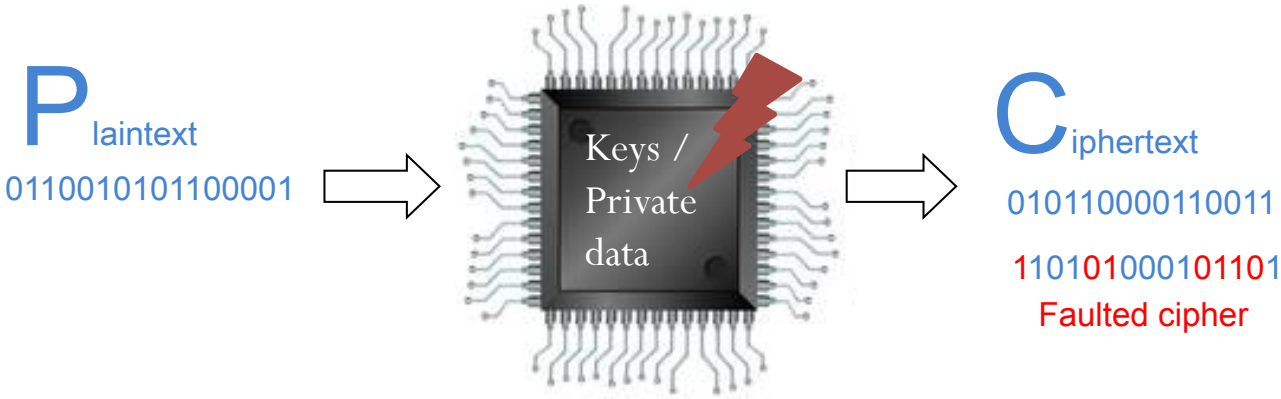
Ecole Nationale Supérieure des Mines SAINT-ETIENNE Site Georges Charpak

Secure devices

- Development of the use of secure devices
- Need of security for critical applications
- Cryptographic algorithms implantation
- Development of attacks to retrieve the secret information

Use of a secure devices

Fault injection in cryptographic devices

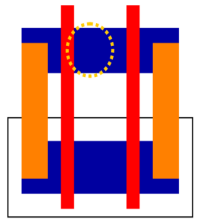
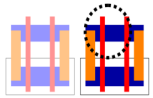
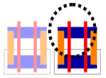
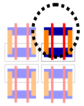


- Security bypass
- Differential fault analysis
  - Ciphering of a plaintext
  - Disruption of the circuit during the ciphering (same plaintext)
  - Comparison between Ciphertext and faulty ciphertext (attack)
  - Information about the secret key

Laser injection

- Mean of fault injection
- High spatial accuracy (1µm spot size)
- High timing accuracy (from s to ps illumination time)
- Allows to perform powerful fault attacks

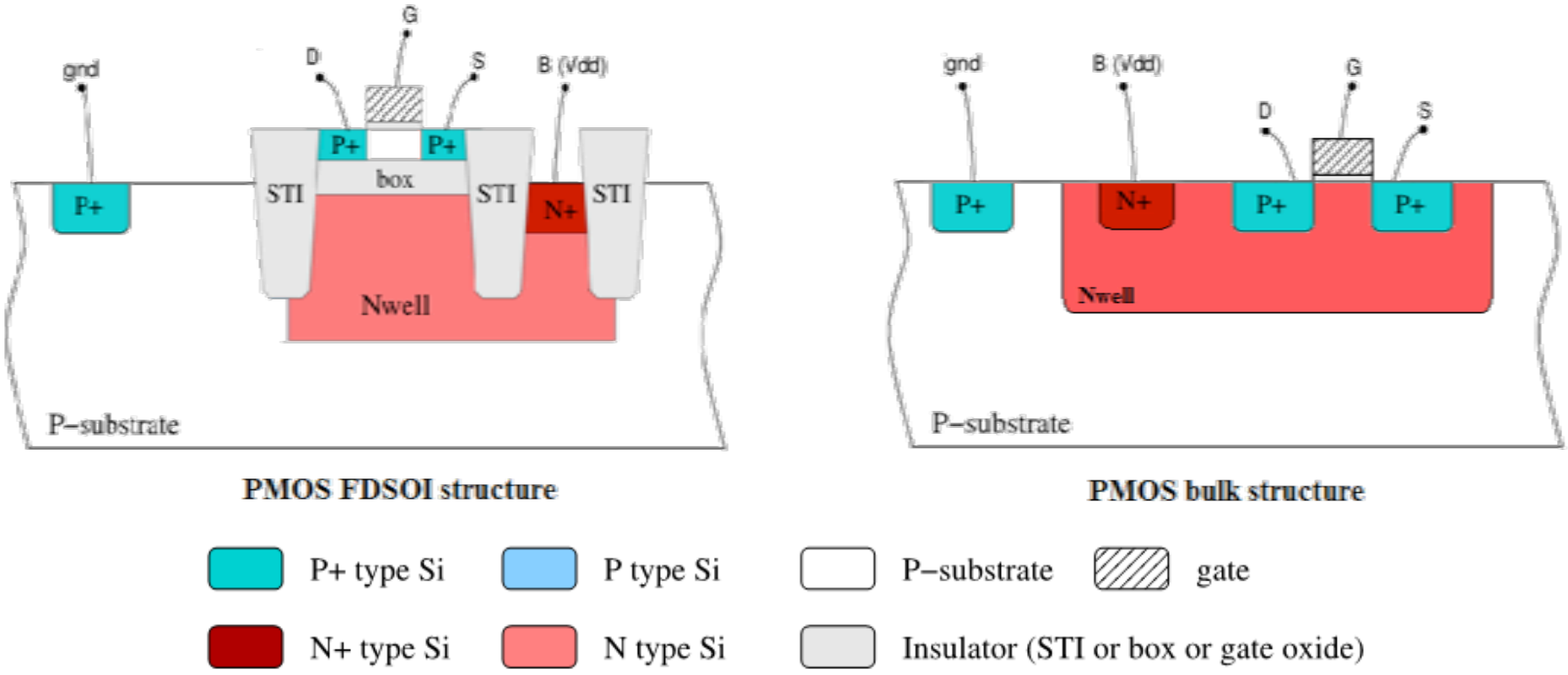
- (Very) expensive
- Preparation of the circuit

	Transistor	SRAM Cell
350nm		
130nm		
90nm		
65nm		

Transistor technology nodes compared to a ø1µm laser spot size

Laser beam ø1µm and its area of effect

28nm PMOS structure: Bulk and FDSOI



Outline

- Introduction
- FD-SOI/Bulk sensitivity to laser injection
- Conclusion

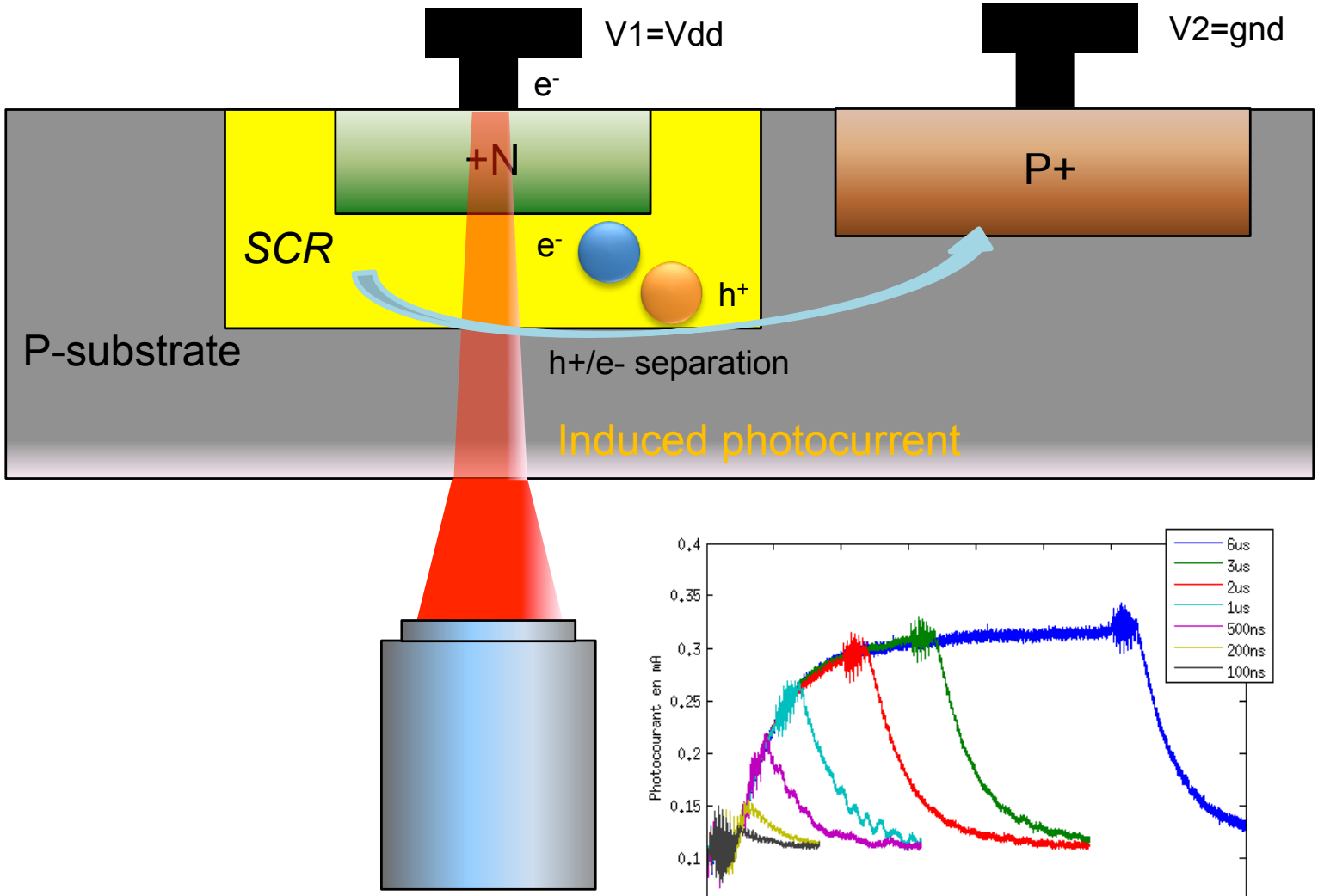
Introduction

LIESSE project

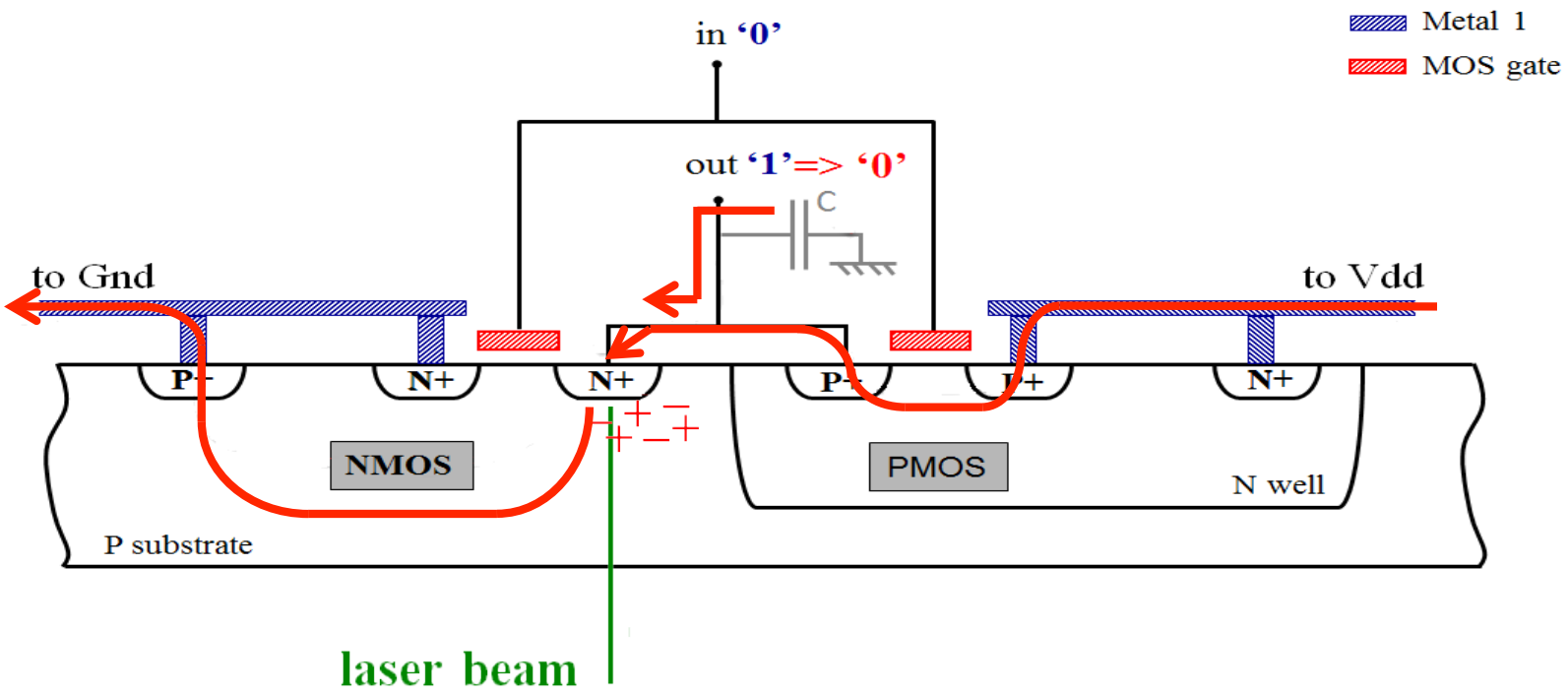
Aim of the project:

- Tool development for safety assessment against laser injection on integrated circuit
  - Certifications
  - Countermeasures

Photoelectric effect

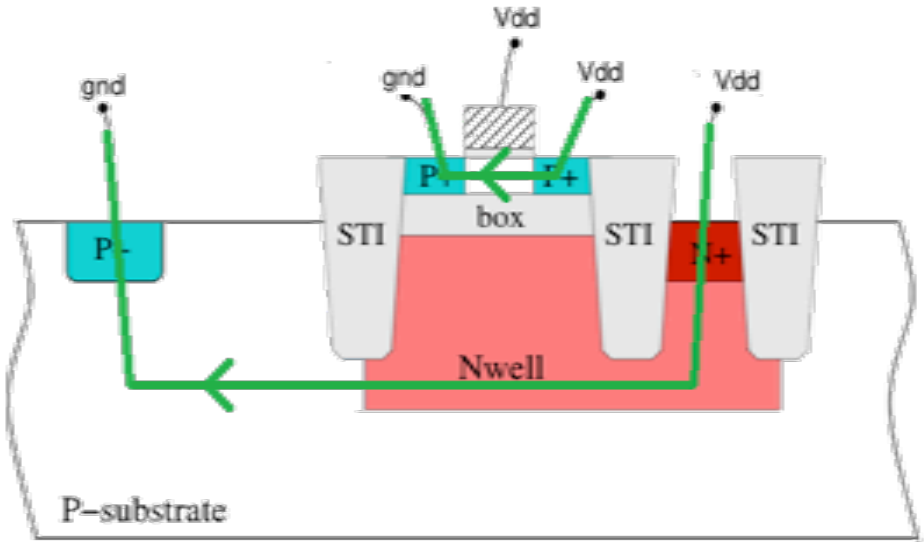


Laser fault injection mechanism

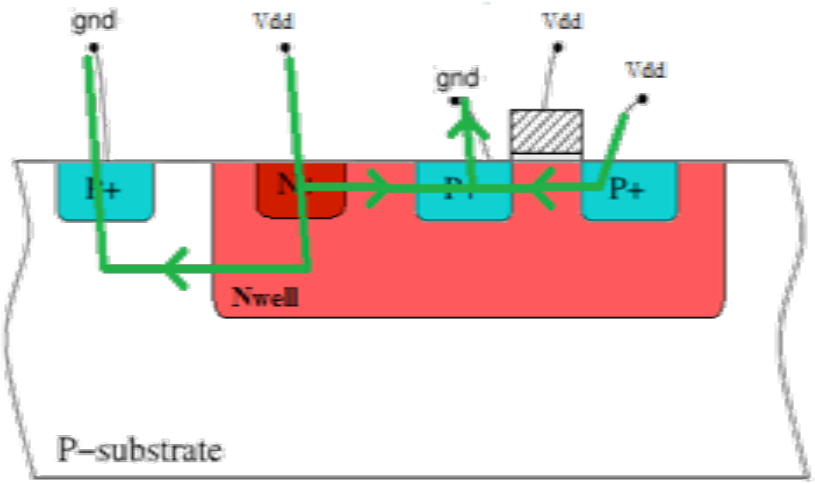


- Inverter sensitive area: drain of the blocked MOS
- Transient change of logic state - Fault

Charge's generated volume depending on the structure



PMOS FDSOI structure

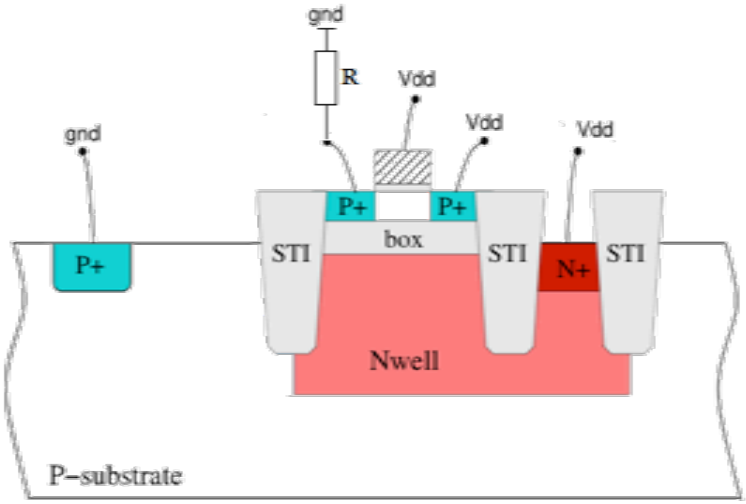


PMOS bulk structure

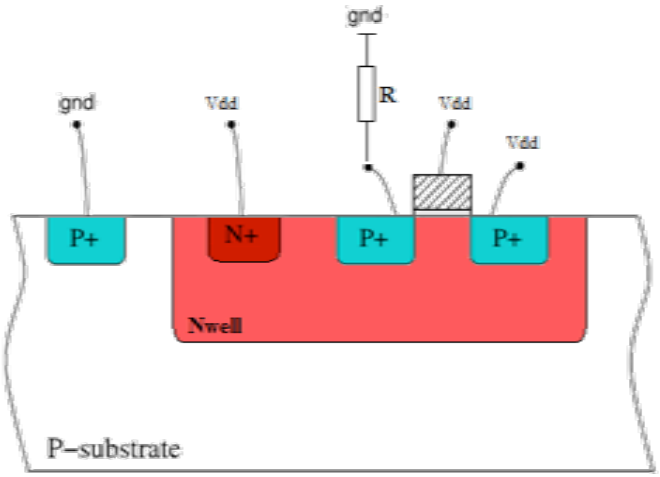
	PMOS FDSOI	PMOS Bulk
Effective volume charge	Channel	Channel + Substrate + Nwell
Induced current	From drain to source + Nwell to substrate	From drain to source + Drain to substrate +Nwell to substrate

FD-SOI/Bulk sensitivity to laser injection

Measurement circuit



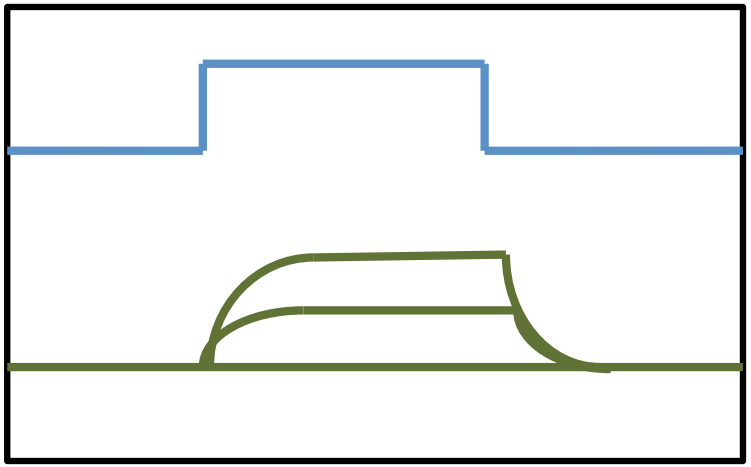
PMOS FDSOI structure



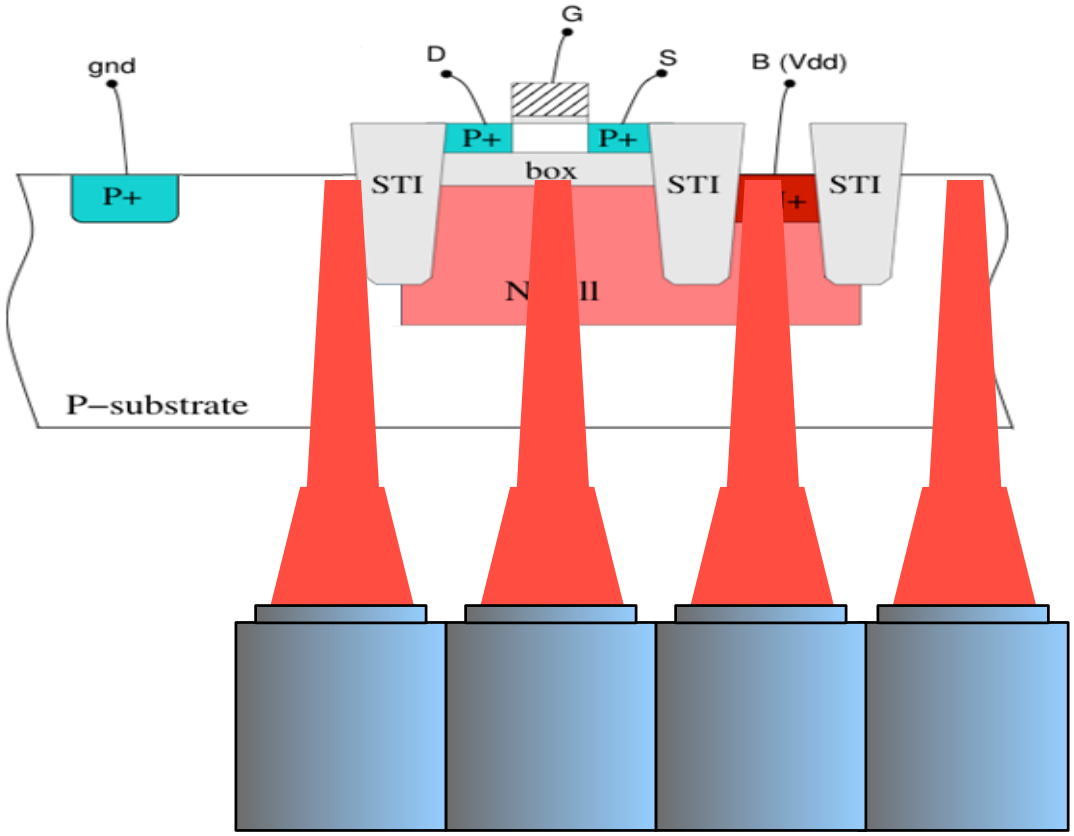
PMOS bulk structure

- Measurement of the maximum induced current flowing through the transistor
- For FDSOI, drain and source currents are equivalent

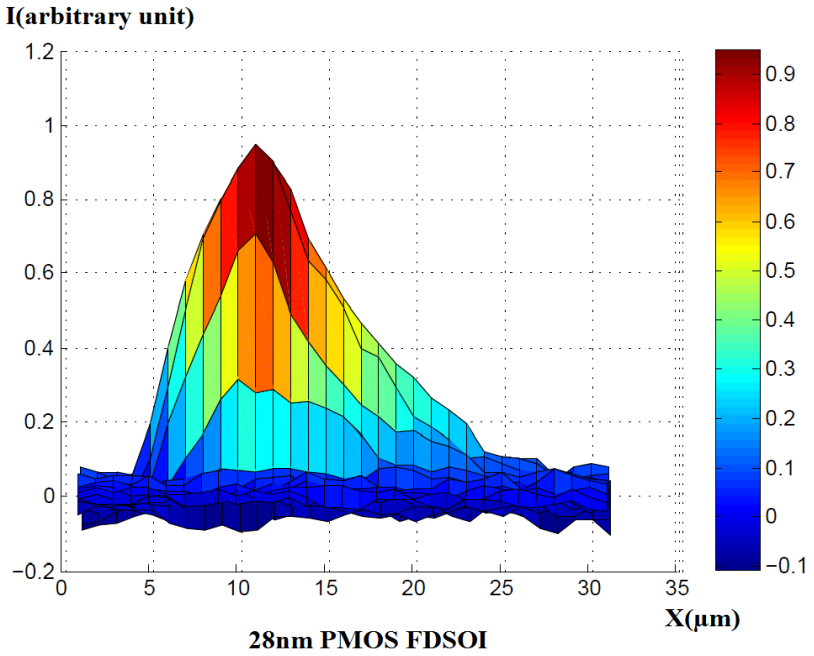
Laser injection measurement

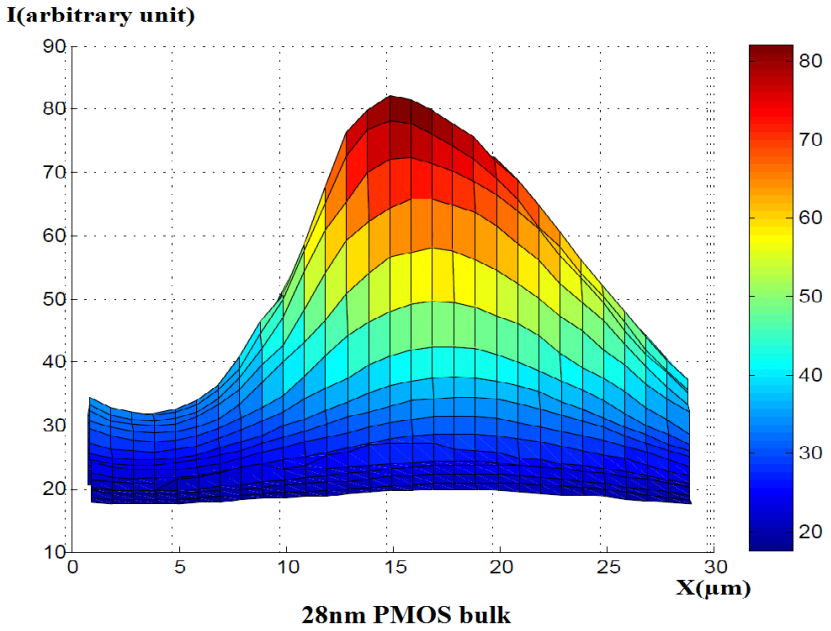


Induced current vs Time



FD-SOI vs Bulk (28nm)





I_{max}=1a.u

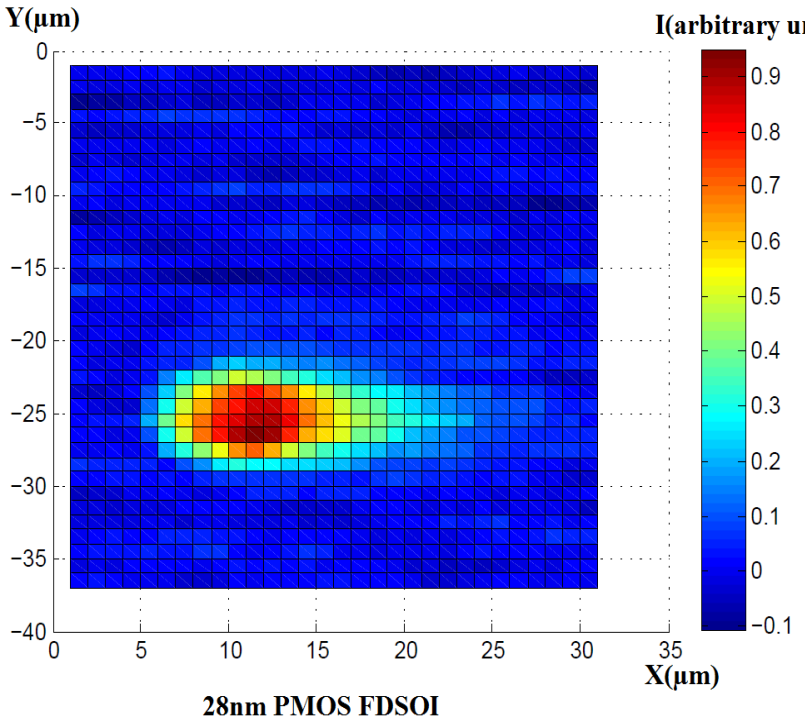
I_{max}=80a.u

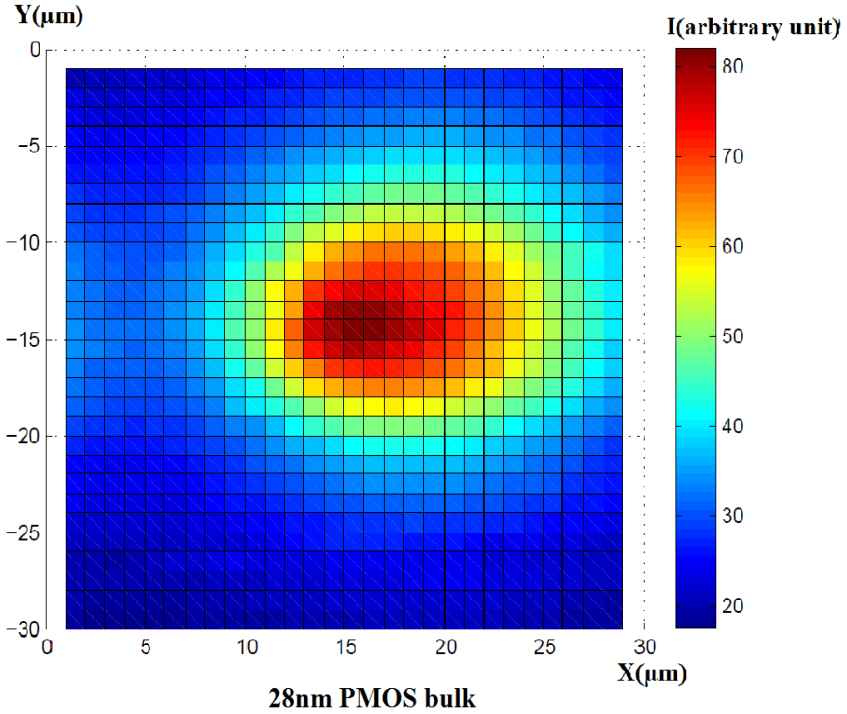
- NMOS (W,L): 1μm*3μm

Spot size: 1μm*1μm

➢ **Amplitude of induced current: x80 between bulk and FD-SOI**

FD-SOI vs Bulk (28nm): box effect





A=5µm*4µm

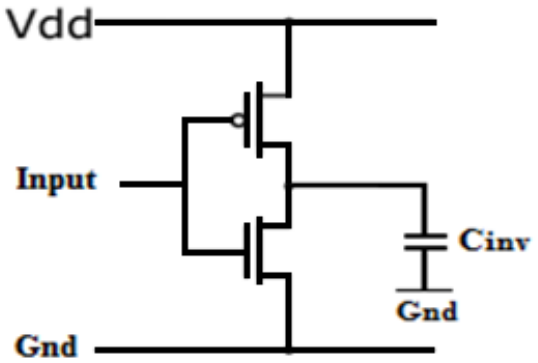
A=13µm*12µm

- **Less transistors are affected by the laser with FDSOI technology**

Capacitance charge

- Worst case injection
  - Only drain current considered
  - No compensation with other currents

➢ **Logic state more difficult to change with FDSOI**



	FDSOI	Bulk
Laser induced current amplitude	1a.u	80a.u
Capacitance charge current	0,2a.u	9a.u

Conclusion

Conclusion

- FDSOI advantages:
  - Charge generated volume small due to insulation between channel and substrate
  - Reduction of the long distance effect of the laser due to the insulator box

- FDSOI seems to be a good solution for secure circuit implementation

Questions?