20/11/2025

BITFLIP

Optical probing on custom bench

THALES
Building a future we can all trust

ALPhA NOV
Centre Technologique Optique et Lasers

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

DGA
DIRECTION GÉNÉRALE DE L'ARMEMENT

- Introduction
- Context, objectives
- EOFM/EOP techniques
- State of the art (attacks, constraints, countermeasures)
- Experimental results and rating
- Conclusion

Subject and purpose

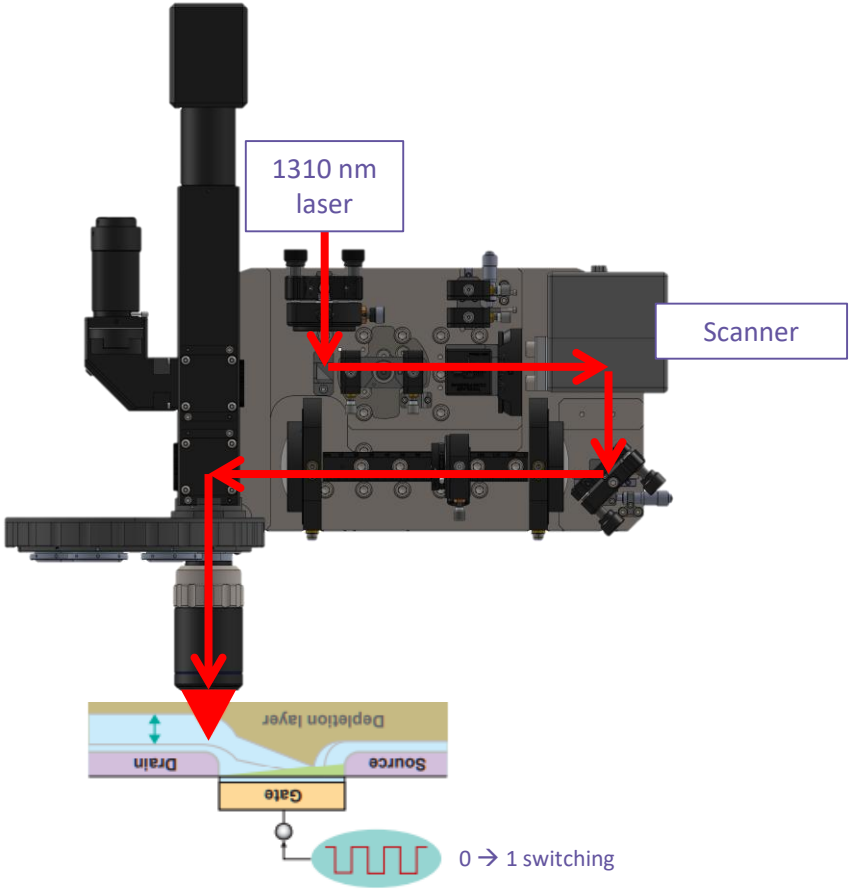
- Faced with the growing interest of Electro Optical Frequency Mapping (EOFM) and Electro Optical Probing (EOP) in this type of means, DGA wanted to acquire the skills and means of spatial and temporal functional analysis of electronic chips, through a demonstrator.
  - Check university publications versus reality
  - Check state threats, state of the art published security in these domains
  - Go beyond existing work, anticipate the threat
    - Know the level of confidence of security mechanisms into ASIC, FPGA, memories, ...
    - Tomorrow (>10/20 years) : anticipating technological developments and new threats to ensure lasting protection.

- But we have a problem with this type of expertise :
  - Safety ≠ Security
  - White box ≠ black or grey
  - Hardware and software is not appropriate to extract sensitive data from a secure electronic component in black box.

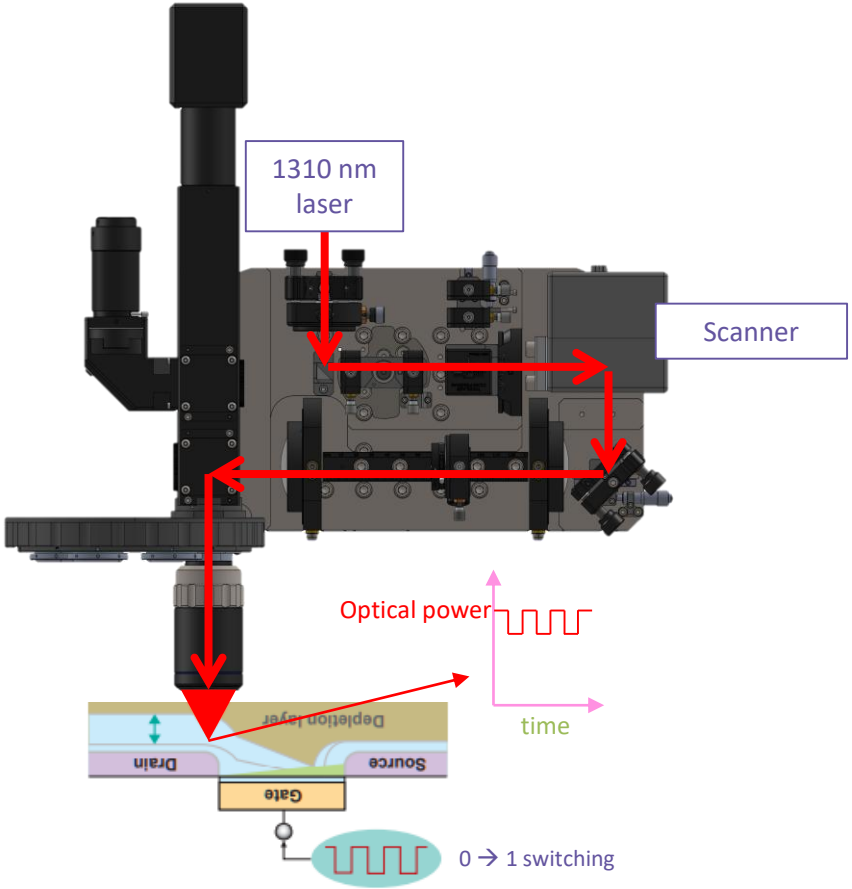
Objectives

- Develop a demonstrator and a new physical attack modality using optical probing
- Adapted to cyber needs, state-of-the-art, open architecture and evolvable (hardware and software)
- Reproduce an university attack into a Xilinx Kintex 7 FPGA using optical probing 28 nm technological node
  - Alphanov and Thales present this demonstrator and the first results
- and more…

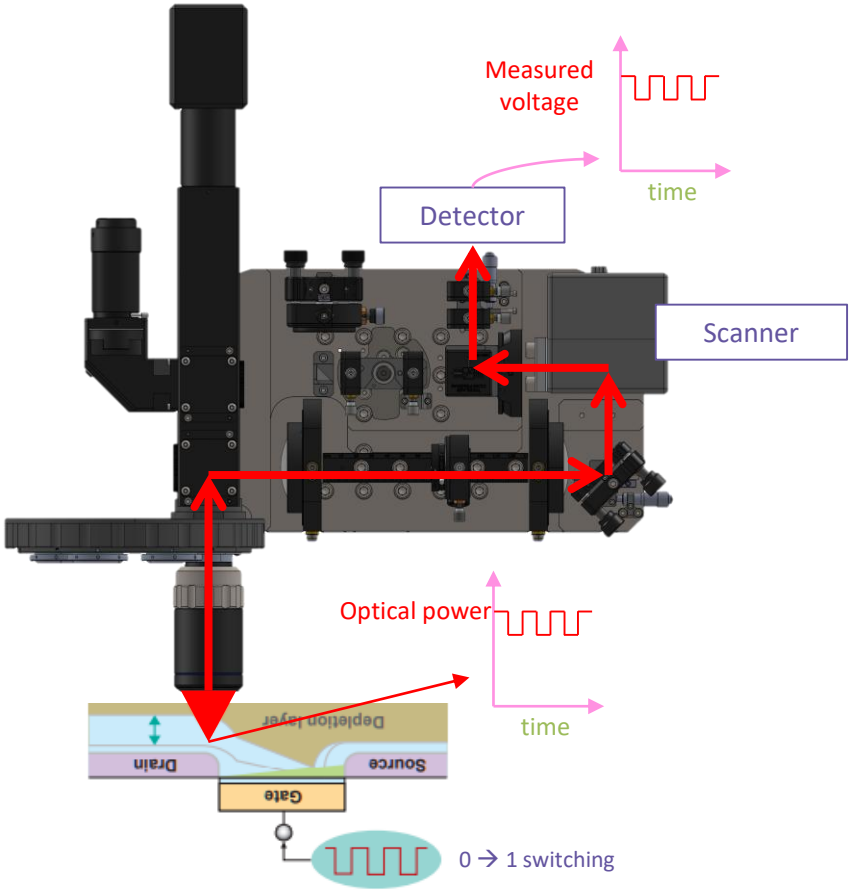
EOFM and EOP techniques

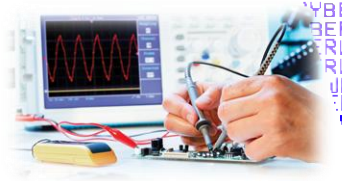


EOFM and EOP techniques

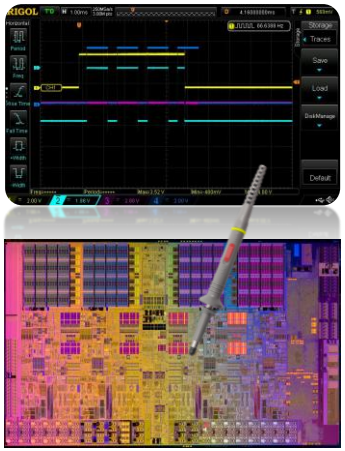


EOFM and EOP techniques



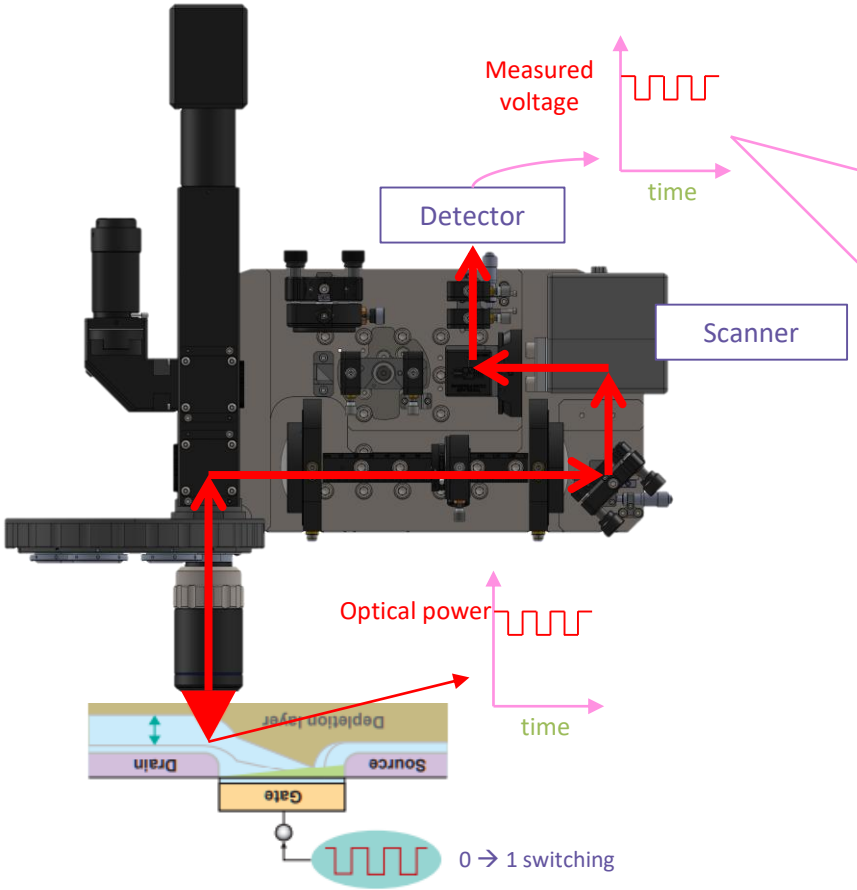


by analogy



Comparison with an oscilloscope

EOFM and EOP techniques



EOFM

Spectrum Analyzer

EOP

Oscilloscope

Electro Optical Frequency Mapping (EOFM)

- Laser scan on an area of interest
- The measured signal at the frequency of interest is calculated by the spectrum analyzer
- Reconstruction of a map with the active areas of the component

"On the Power of Optical Contactless Probing: Attacking Bitstream Encryption of FPGAs", Shahin Tajik, Heiko Lohrke, Jean-Pierre Seifert, et Christian Boit, Université de Berlin (2018)

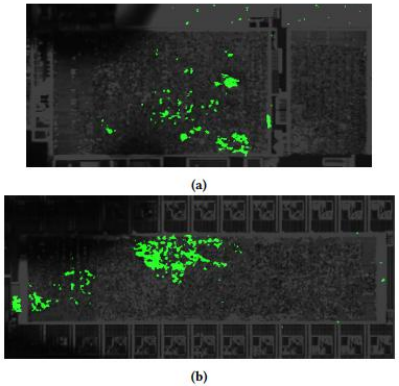


Figure 12: Activity map at the plaintext data frequency (CCLK/256) revealing gates potentially carrying the decrypted bitstream data. (a) "Main" logic area. (b) "AES" logic area. The leftmost edge of the AES area shows activity that might indicate an output port.

Step 1/EOFM : frequency mapping (showing activity zones)

Electro Optical Probing (EOP)

- 1-point attack
- Static measurement
- Signal evolving in time
- Direct reading of the information by the oscilloscope

"On the Power of Optical Contactless Probing: Attacking Bitstream Encryption of FPGAs", Shahin Tajik, Heiko Lohrke, Jean-Pierre Seifert, et Christian Boit, Université de Berlin (2018)

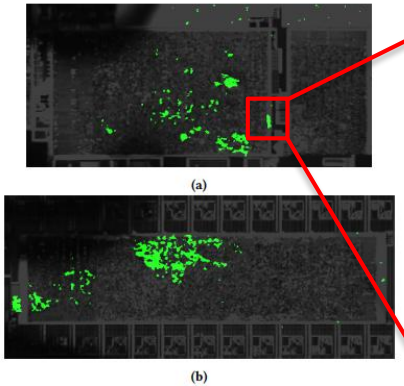


Figure 12: Activity map at the plaintext data frequency (CCLK/256) revealing gates potentially carrying the decrypted bitstream data. (a) "Main" logic area. (b) "AES" logic area. The leftmost edge of the AES area shows activity that might indicate an output port.

Step 1/EOFM : frequency mapping (showing activity areas)

f_{clock} : 3-33 MHz

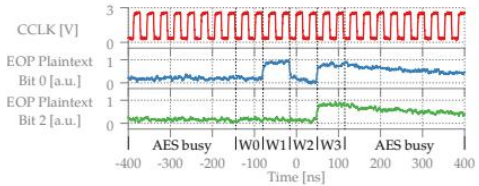


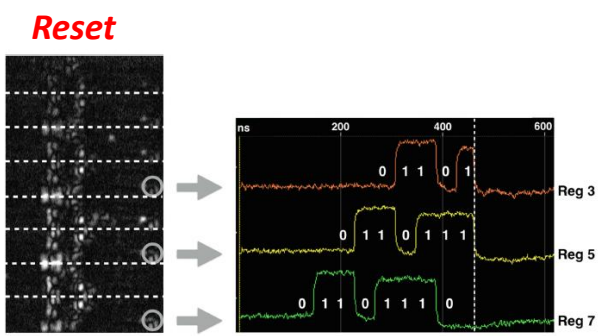
Figure 15: Optically extracted plaintext data for two bus lines of the 32-bit plaintext data bus as well as the CCLK signal. The plaintext bitstream data was 0101 for bit 0 and 0001 for bit 2. W0 to W3 denote the "data valid" time slots for word 0 to word 3 on the plaintext bus.

Step 2/EOP : 1-point dynamic probe (acces to information)

State of the art - Security

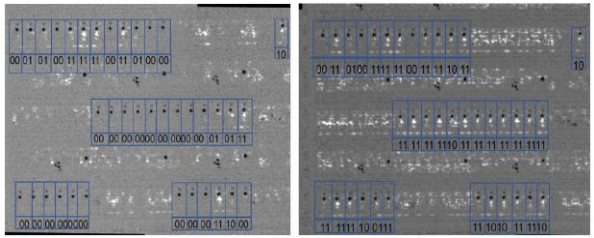
Reverse of naive PUF FPGA implementation

- Altera Cyclone IV 60nm
- Red key value recovery with EOFM
- Red key value recovery with EOP
- Output of PUF with frequential / EOFM / EOP



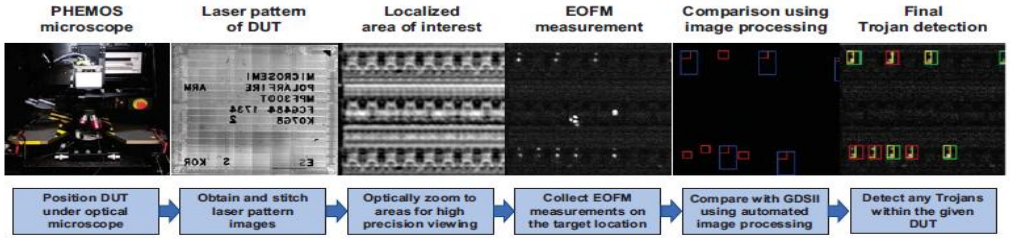
Reverse engineering of a logic locking mechanism

- Microsemi Polarfire FPGA 28nm
- Logic locking key value recovery with EOFM
  - Design clock frequency / Reset clock frequency



Identification of Trojan horse in FPGA fabric

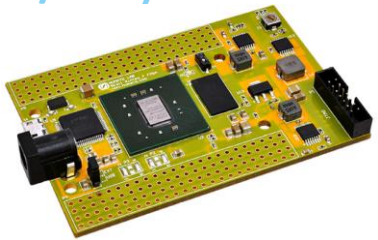
- Microsemi Polarfire FPGA 28nm
- Comparative analysis EOFM

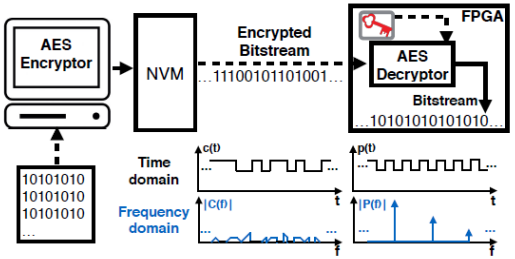


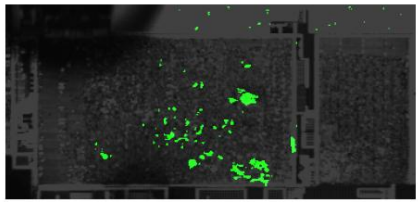
State of the art – Bench validation

Reverse of cryptographic hardware bloc (EOFM/EOP)

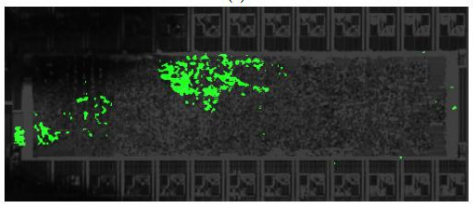
- Kintex 7 / 28nm
- Plain text bitstream value recovery
- Creation of artificial frequency in bitstream
- Identification of cryptographic bloc output bus
- Data bus recovery

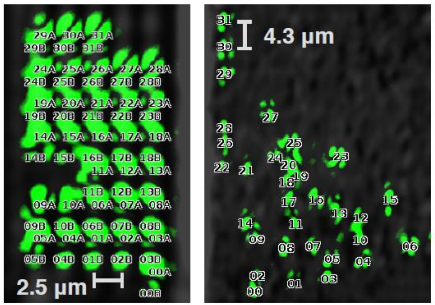


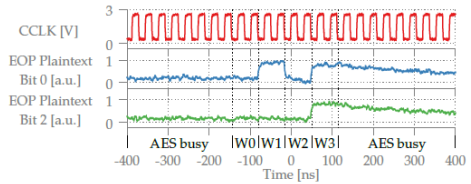




(a)







State of the art – Constraints

Technological node

- Spatial precision is dependant of wavelength and Numerical Aperture

$$R_{(Rayleigh)} = 0.61\frac{\lambda}{NA}$$

NIR is good for…

	Technology node				
	32nm	22nm	14nm	10nm	7nm
Lens NA	1.4 (LIO)	2.6 (SIL)	3.0 (SIL)	3.3 (SIL)	TBD
Optical resolution @ λ = 1500 nm	654 nm	352 nm	305 nm	277 nm	TBD – new solution needed
@ λ = 1064 nm	464 nm	250 nm	216 nm	197 nm	TBD
Contacted gate pitch	112.5 nm [2]	90 nm [3]	70 nm [1]	~64 nm [4]	~50 nm [4]
FI capability	Fair	Very good	Good	Fair	TBD

- Wavelength decrease
  - Photoelectric effect => signal disturbance (noise, fault injection)
  - Silicon absorption => silicon thickness < 10µm
- NA increase (air = 1) / Must be close to Si (3,4 for 1064nm) => SIL lens
- 550nm + SIL GaP => optimal theoretical resolution 80nm

State of the art – Constraints

- Node dimension contraints could be relaxed:
  - Contacted gate pitch is more pertinent to consider and larger than node dimension
  - Spacing between the areas of interest is related to integrated circuit design and could be greater than contacted gate pitch

Process technology

- Bulk
  - Most of the recent papers on security topics target 28nm bulk component (Polarfire FPGA, Xilinx Serie 7)
- FinFET
  - Similar results between bulk and FinFET were demonstrated in academic papers
  - Results were obtained experimentaly at ITSEF on 16nm FinFET
- SOI
  - Some limitations (using photoelectric source, sample preparation, etc…) but possible
  - Signal strength could be impacted

State of the art – Constraints

Back side access / Si thinning / power domain access

Frequency of interest (EOFM)

- Frequency analysis
  - Electromagnetic emanations
  - Current consumption
  - Frequential optical probing

Signal access to trigger loop (EOFM/EOP)

- Not systematic for EOFM analysis if signal of interest is continuous

Signal access to trigger acquisition (EOP)

- Electromagnetic emanations/Current consumption + pattern matching

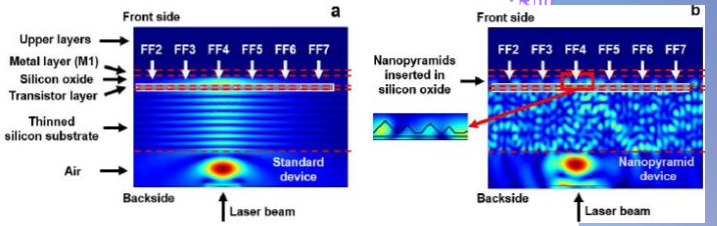
No jitter (EOFM/EOP)

- Frequency stability allows to limit the frequency bandwidth and then limit signal noise(EOFM)
- Too much jitter would lead to null signal or at least bad SNR when averaging (EOP)

State of the art – Countermeasures

Circuit specific countermeasures (research literature)

- Thermic effect wavelength detection (above 1100nm) => Structures sensitive to temperature
- Thinning/opening detection
- Reflected signal jamming

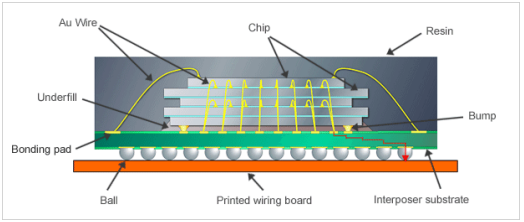


Design specific countermeasures (research literature)

- Specific standard cells to limit the usable signal (opposite signal in the smallest area)
- Dual-rail logic and pertient electric implementation (limitation of maximum voltage and swing between maximum and minimum values)

Some non specific countermeasures already exist on secure component

- Secure packaging
- Photonic effect wavelength detection (below 1100nm) => Usual light sensors against fault injection
- Buses / memories encryption
- DPA counter limiting the number of possible resets
- Desynchronisation



Advantages of custom bench for security

Easier hardware upgrade

- COTS parts : easier maintenance and evolutivity at competitive costs
- Hardware adaptability depending on test needs (laser source, SLED source, amplification, photodiode)

Easier software upgrade

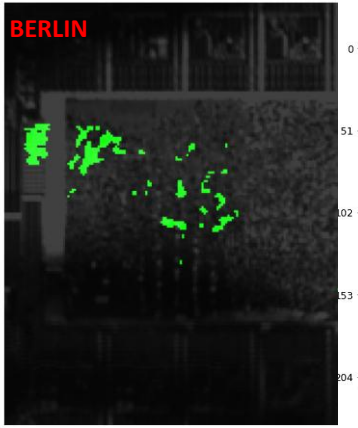
- Total control of software environment
- Simplified bug fix
- New features depending on needs

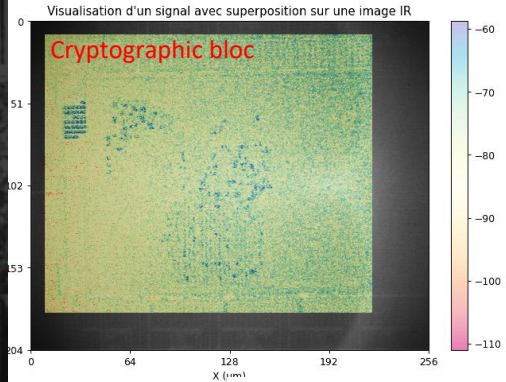
Flexibility

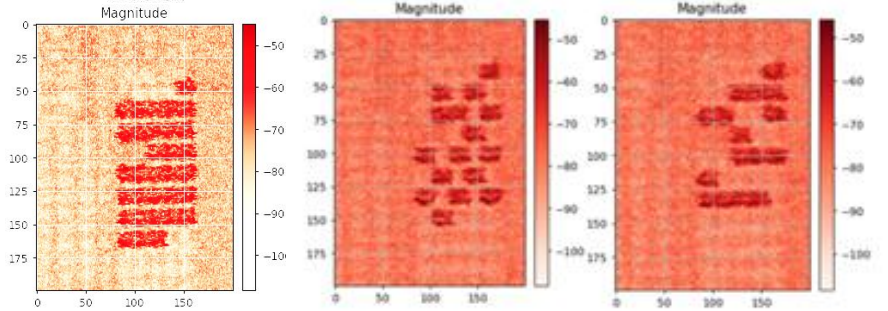
- Instrumentation in potentially complex test scenarios
  - EOFM scan automation on parameters (Z focus, frequency, laser power, etc…)
  - EOP automation on multiple points of interest with modification of oscilloscope parameters (trigger, etc…)

Experimental results on Kintex 7 (Skoll Numato – 50µm)

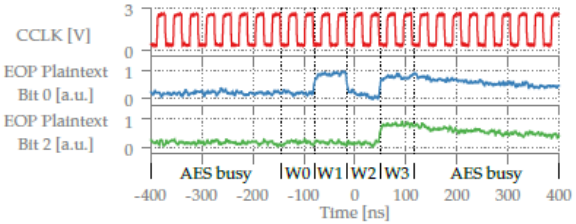
EOFM comparison

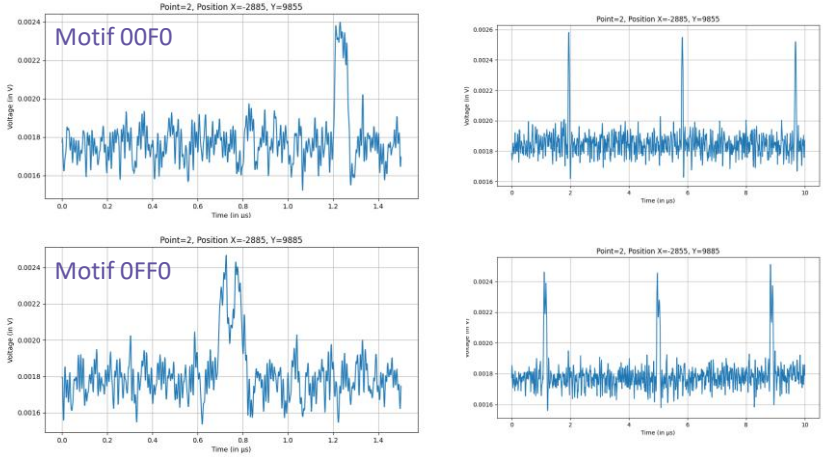


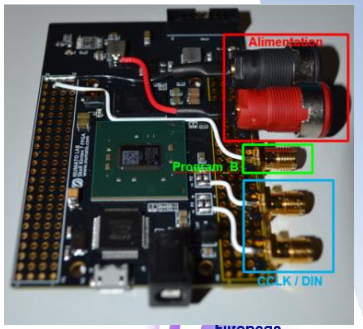




EOP comparison







Experimental results on Kintex 7

JIL Rating

Factor	Identification		Exploitation	
Time elapsed	**5** (> 1 month)	Sample preparation (thinning). Hardware setup with modification of evaluation board (bitstream load loop, frequency signal, etc…). Software setup to modify bitstreams to identify targeted bus. Identification of the area of interest for EOFM analysis. EOP traces acquisition. Post-treatment of EOP traces to recover logical data.	**6** (< 1 month)	Sample preparation (thinning). Hardware setup with modification of evaluation board (bitstream load loop, frequency signal, etc…). Identification of the area of interest for EOFM analysis. EOP traces acquisition. Post-treatment of EOP traces to recover logical data.
Expertise	**5** (expert)	Security component expert	**2** (proficient)	Can be performed by an operator
Knowledge of the TOE	**0** (public)	Public documentation.	**0** (public)	No documentation needed.
Access to the TOE	**0** (< 10 samples)	Depends on sample preparation step.	**0** (< 10 samples)	Depends on sample preparation step.
Open samples	**0** (public)	COTS.	**NA**	Not applicable.
Equipment	**5** (bespoke)	Xprep sample preparation, Custom bench.	**6** (bespoke)	Xprep sample preparation, Custom bench.
Total	**15**		**14**	

TOTAL = 29

EAL5 : AVA_VAN_4 →
EAL6 : AVA_VAN_5 →

Range of values*	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

Conclusion

Optical probing and security

- More and more security related publications
- No specific industrial countermeasure yet
- Some contraints
- Very powerful when applicable

Custom security oriented bench

- Less expensive than Phemos or others industrial tools
- More evolutive
- More flexible

MERCI