THALES

EUFANET
European Failure Analysis Network

cnes

Functional analysis with dynamic emission microscopy

Jérôme Di-Battista (Thales), Cyril Leroux (CNES), Martin Hlaváč (Charles Univ.), Philippe Perdu (CNES) , Jean-Christophe Courrege (Thales), Bruno Rouzeyre (LIRMM)

- ***PICA data processing***
  - **Database vectorisation**
  - **Database comparison**
- ***Dynamic mapping decomposition***
  - **Microcontroller case**
  - **FPGA case**
- ***PMT Behavioral analysis on FPGA***
  - **Localization to validation**
  - **Behavior validation**
- ***Conclusion***

- ***Objectives :***

- *Lightening databases*

- *Simplification of the comparison between two databases (Fail/safe)*

- ***Method :***

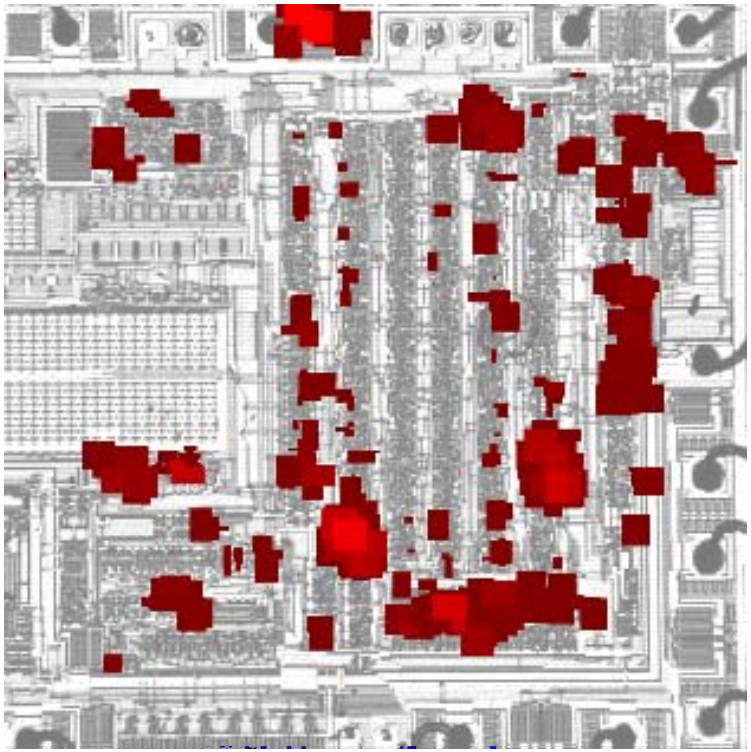
- *Gathering of photons ➔ Creation of events*

- *Each event is defined by :*
  - *spatial temporal coordinates*
  - *Weight*
  - *Max and min coordinates*

- *Second filtering based on the weight of the listed events*

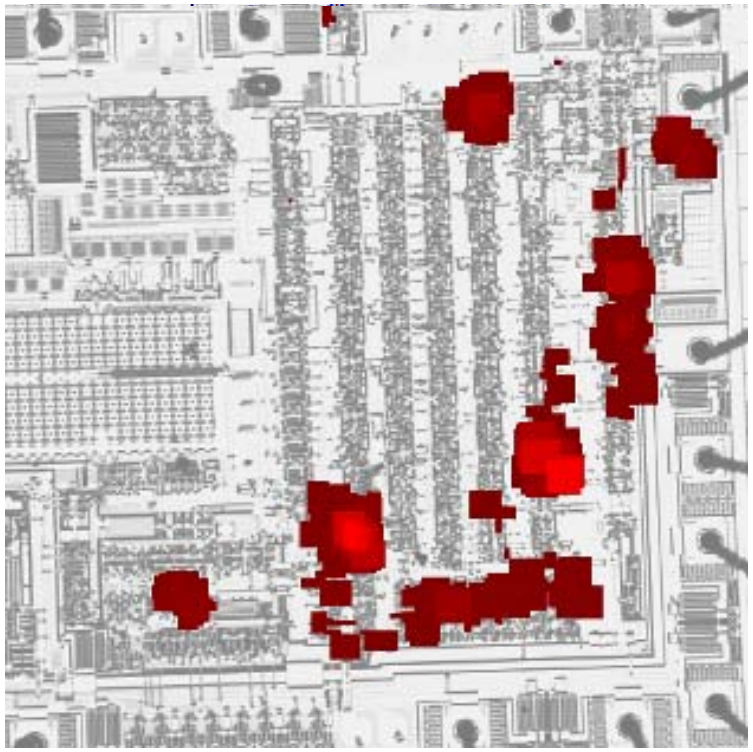
Database Vectorisation

*- In databases, thanks to **PICA** and **STPC** technique, we can obtain a spatio temporal information for each photons acquired.*



Functional ADC

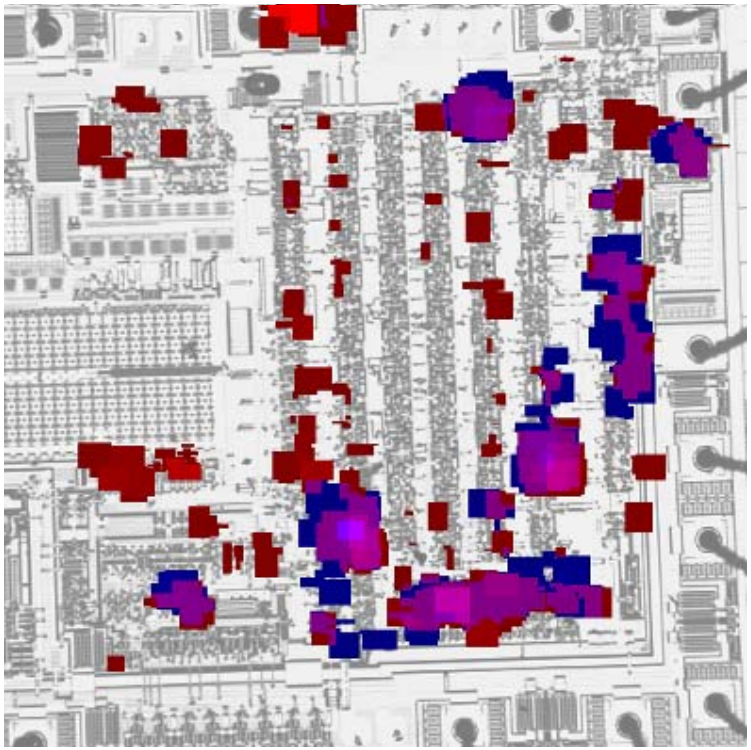
Vectorized and filtered data

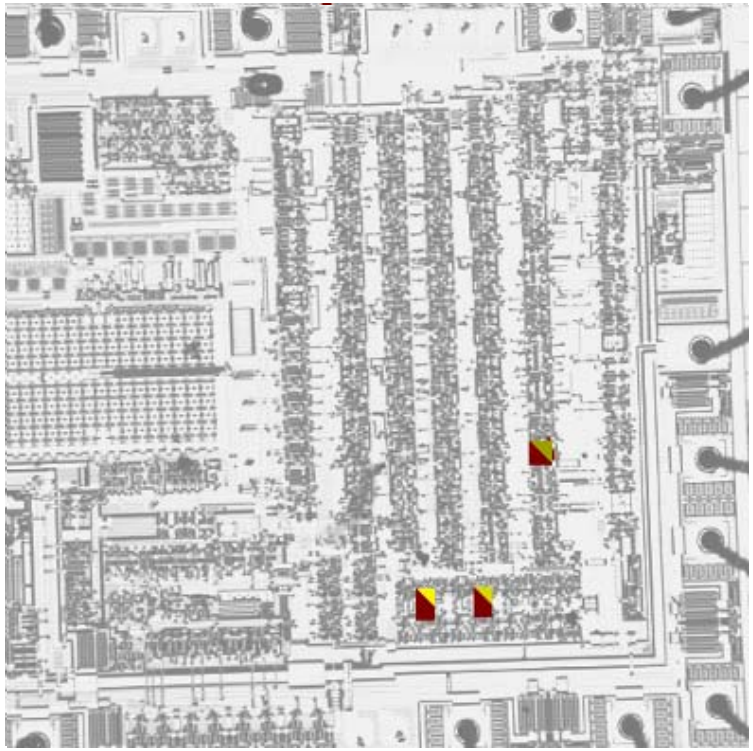


Faulty ADC

Vectorized and filtered data

Database comparison





Events Comparison
1,244 dissimilar events

***Identifying of the failure origin** before the first dissimilar **events**.*

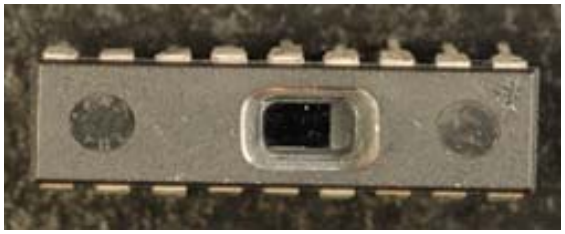
- *PICA data processing*
  - Database vectorization
  - Database comparison
- *Dynamic mapping decomposition*
  - Microcontroller case
  - FPGA case
- *PMT Behavioral analysis on FPGA*
  - Localization to validation
  - Behavior validation
- *Conclusion*

Goal :

- **Decompose the light emission mapping in function of time for try to extract sensible data from a memory.**

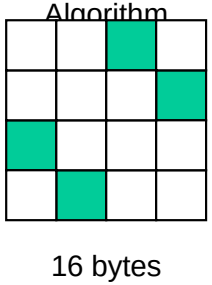
How :

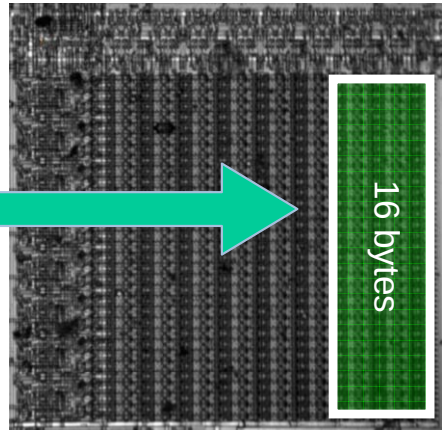
- **Implemention of a « naive » algorithm on a µcontroller (PIC16F84A), to try to recover the secret key through dynamic light emission acquisition**



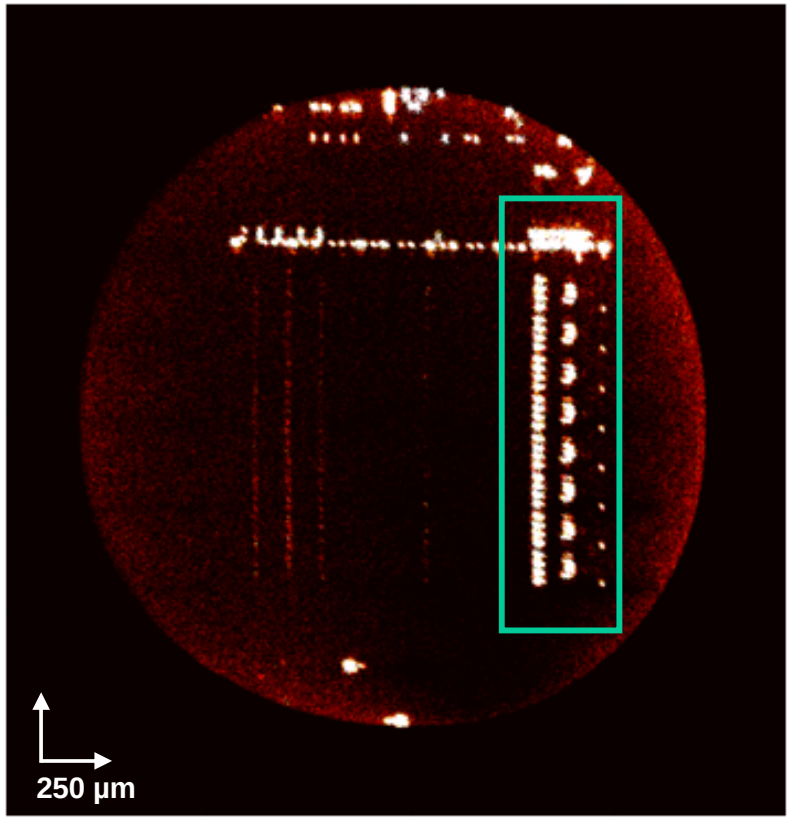
µcontroller open in backside

Measurement Goal





PIC Internal RAM (20x; silicon thickness 40 µm)



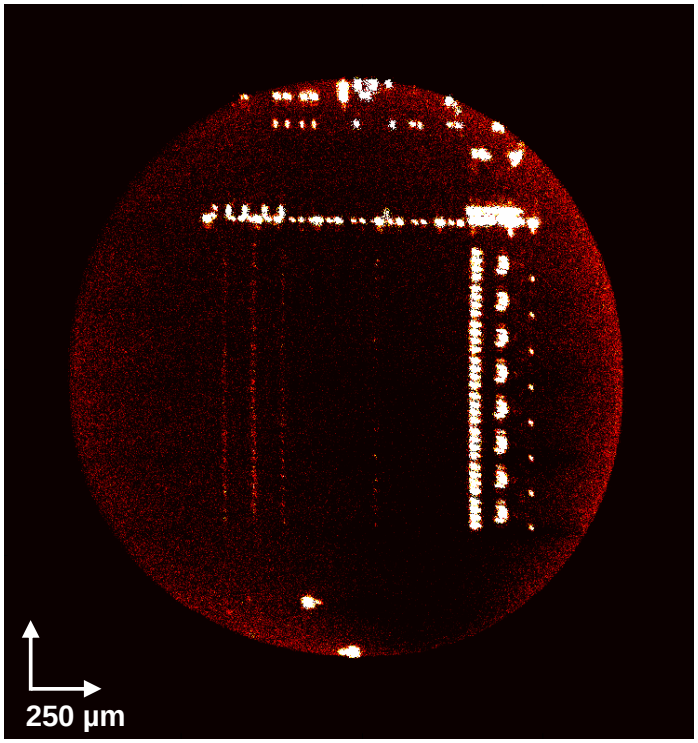
Monitor the changes on the bytes in State block during AES encryptions.

How? *:* **Dynamic light emission detection (Optica)**

Theory **:** byte flips => light is emitted

byte stays => just noise

Static vs Dynamic observation



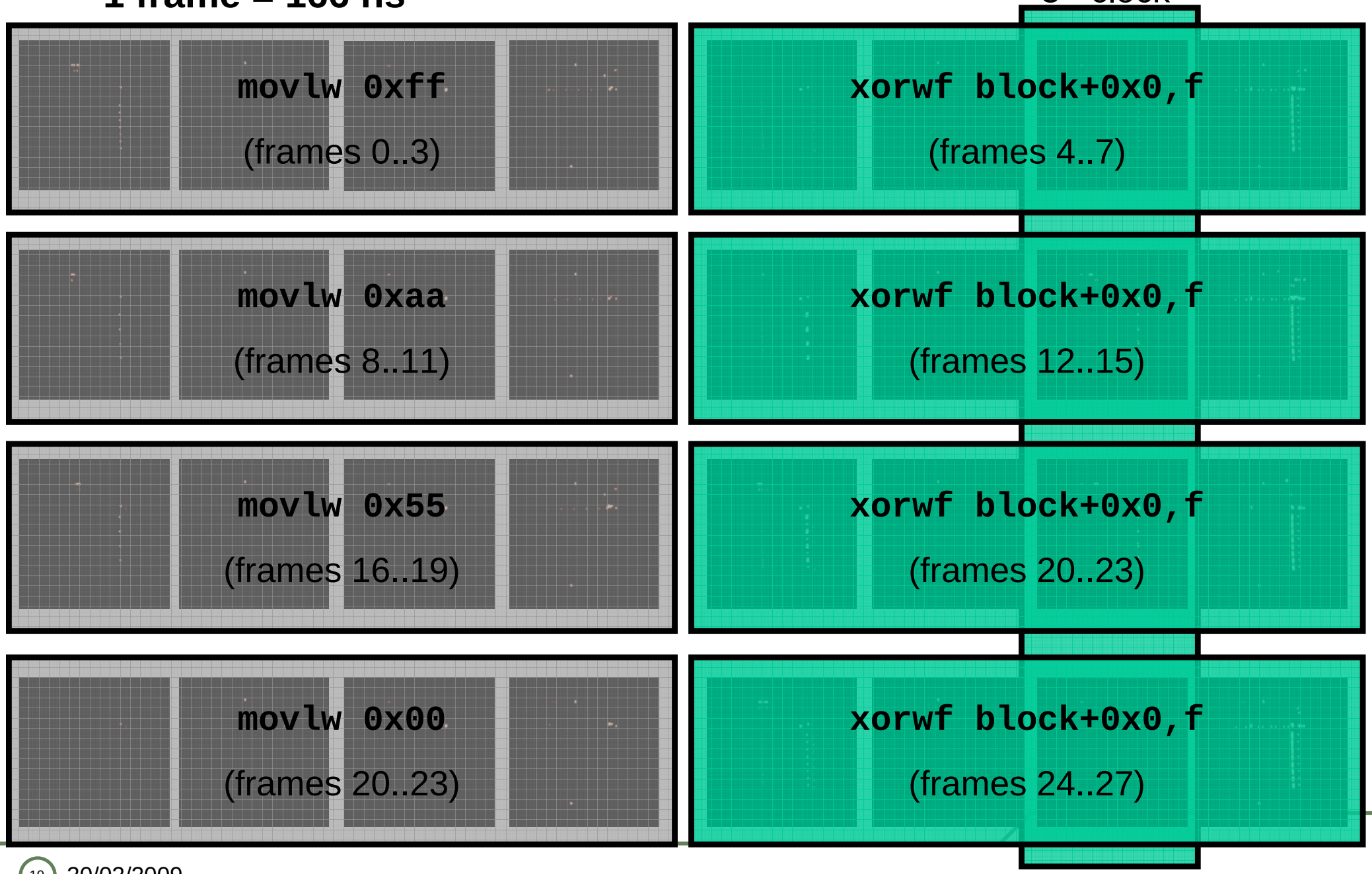
All photons observed in one image

vs.

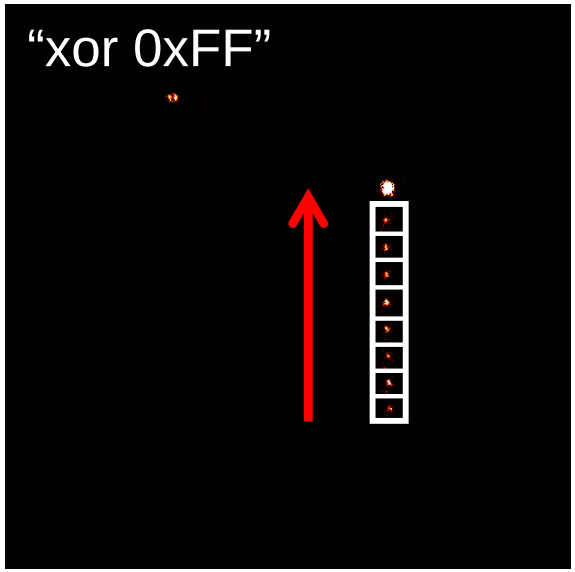
Frames
166 ns = 1 clock cycle

1 frame = 166 ns

3rd clock

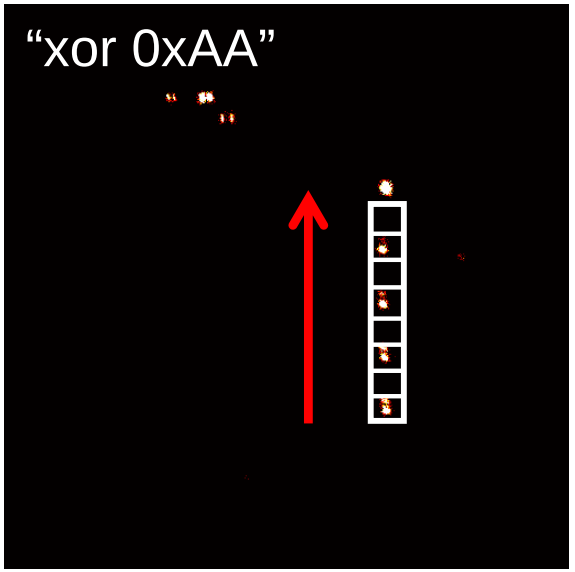


3rd Clocks reveal the key



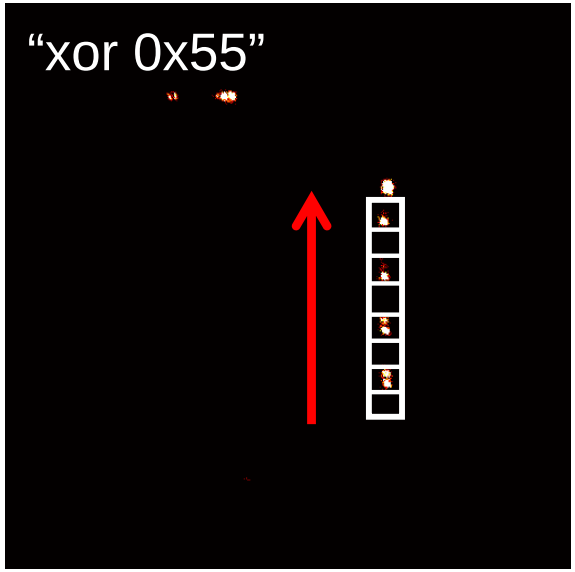
1 1 1 1 **F**

1 1 1 1 **F**



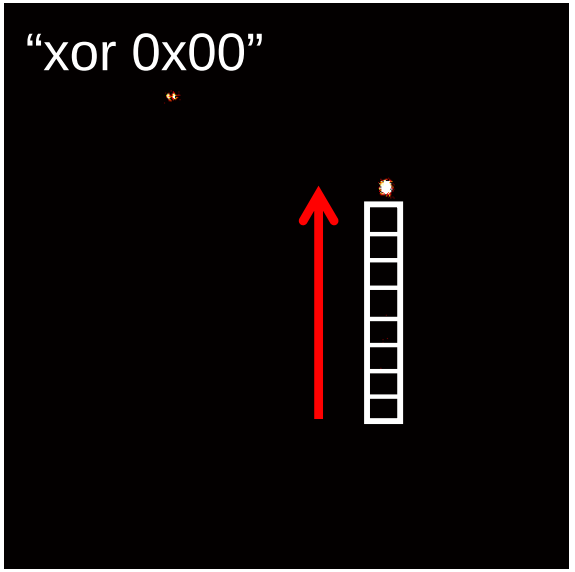
0 1 0 1 **A**

0 1 0 1 **A**



1 0 1 0 **5**

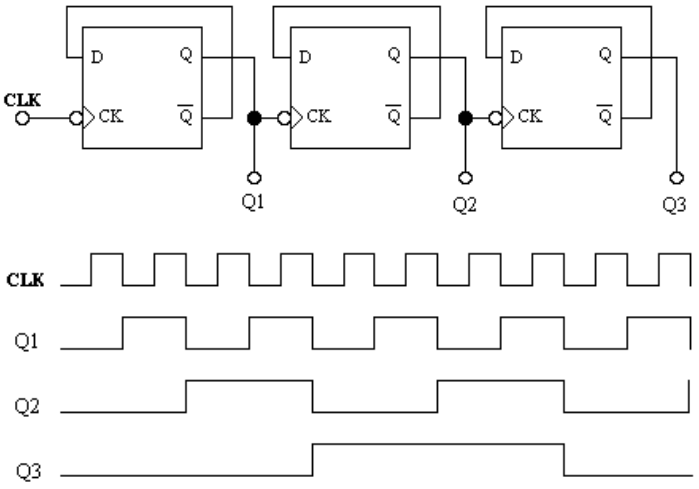
1 0 1 0 **5**



0 0 0 0 **0**

0 0 0 0 **0**

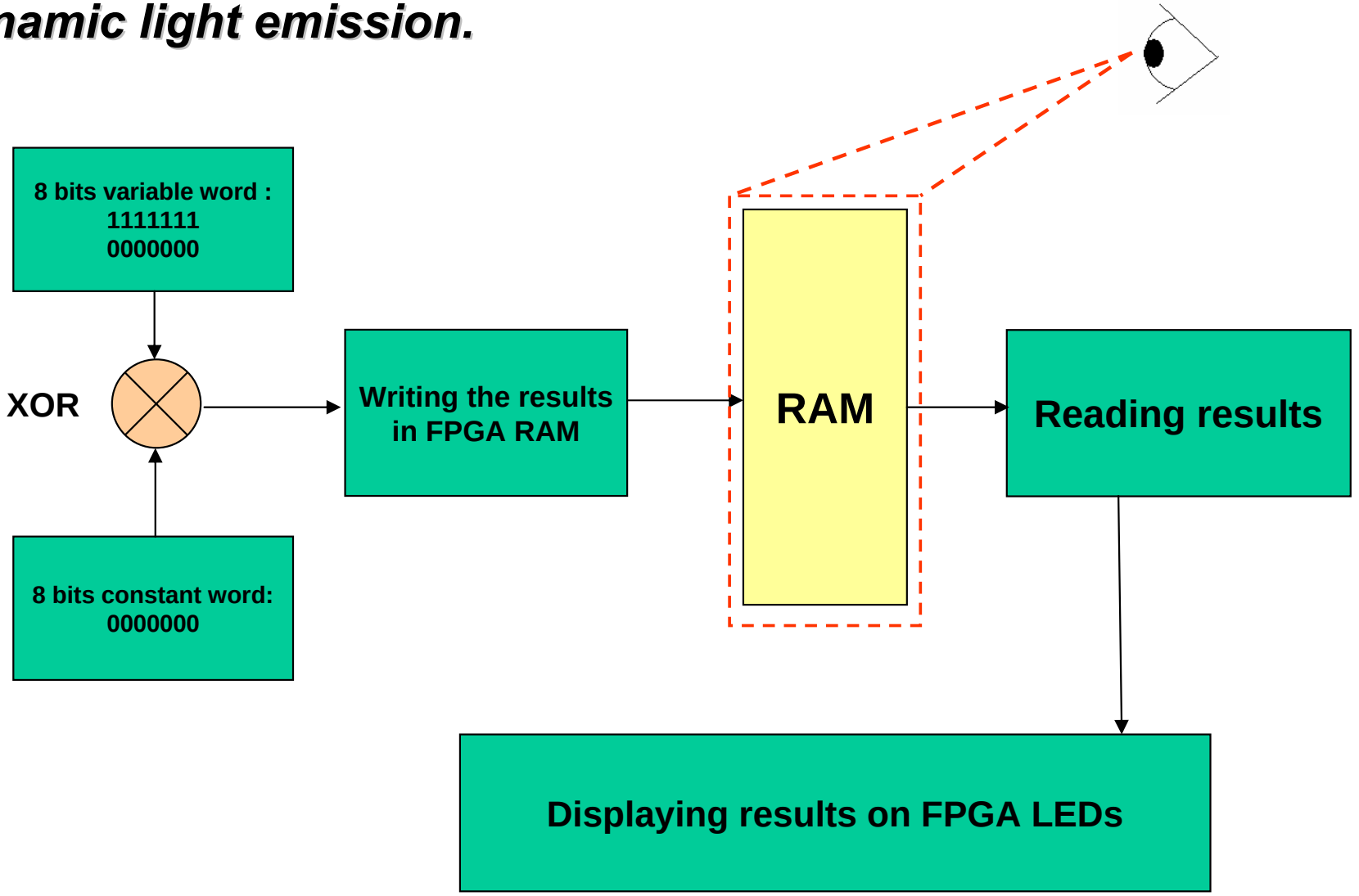
FPGA Application



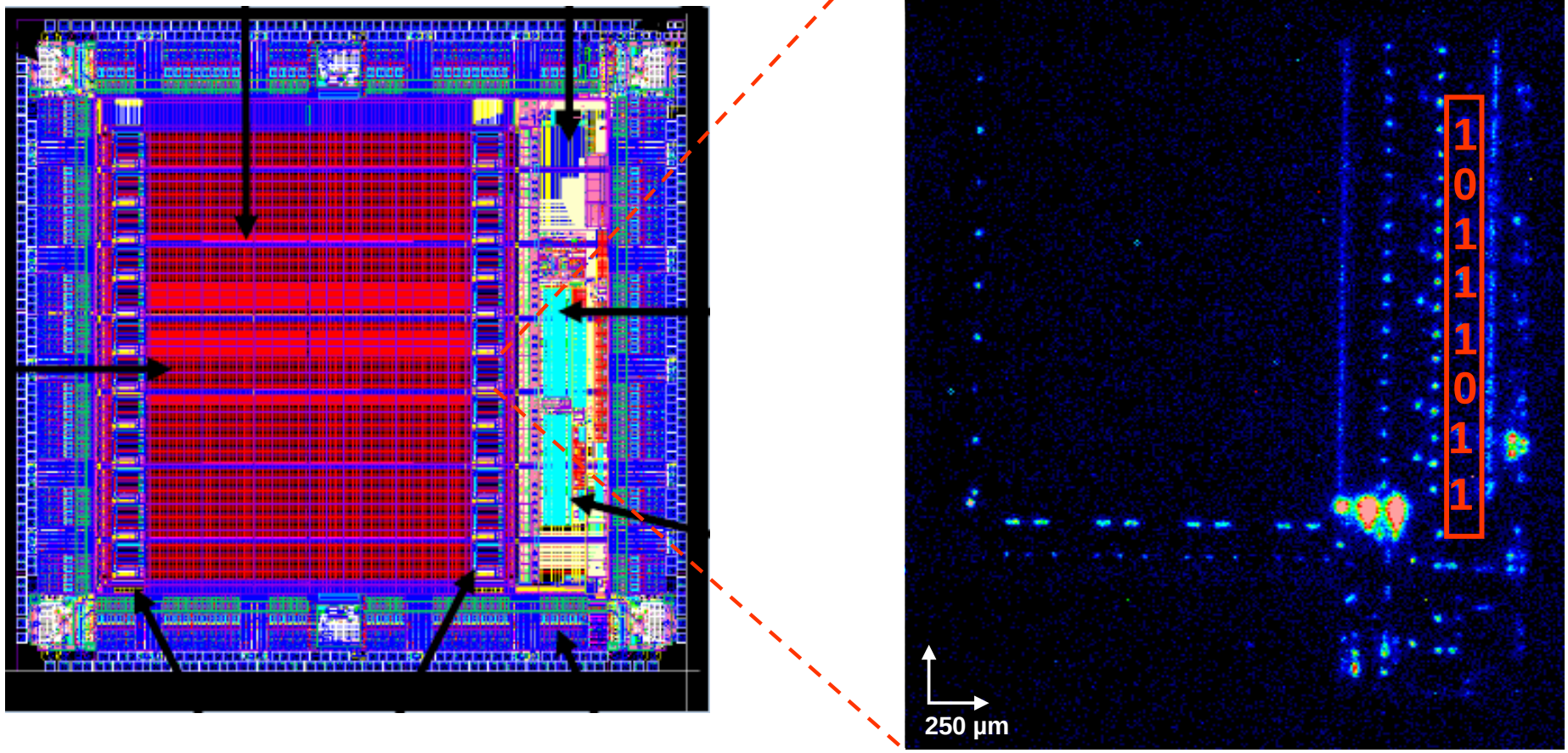
- **Use of an already reprogrammable FPGA opened on the backside**
- **Use of static light emission to localize the area of interest**
- **Use of dynamic light emission technique to determine the function behavior implemented on FPGA**

Access Memory control

- Read output data on internal RAM of FPGA with static and dynamic light emission.



Read / Write 8 bits word **10111011** to adress 0x00

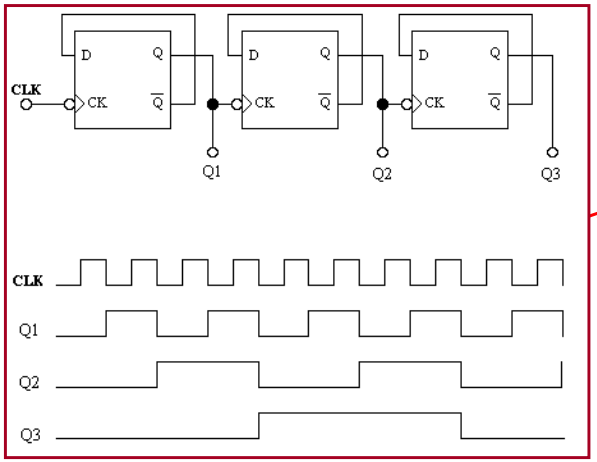


Memory Emission Mapping [20x]

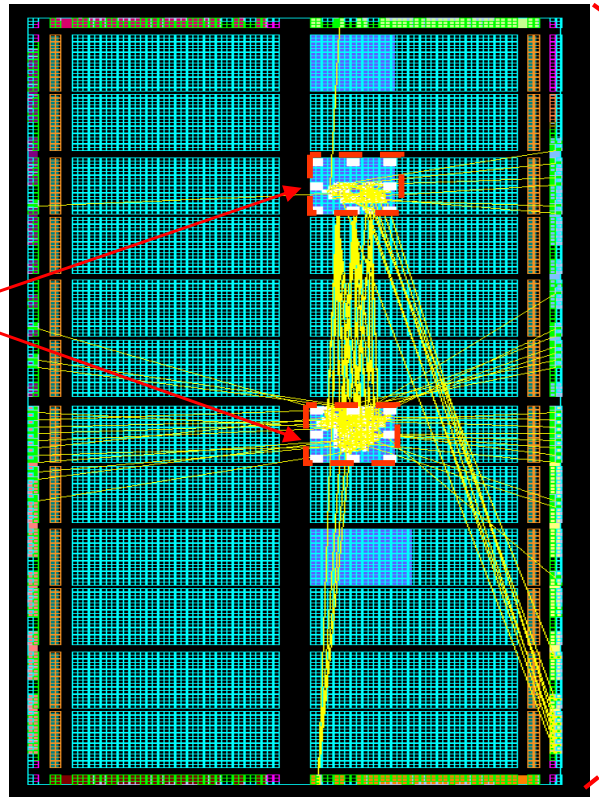
- ***PICA data processing***
  - Database vectorisation
  - Database comparison
- ***Dynamic mapping decomposition***
  - Microcontroller case
  - FPGA case
- ***PMT Behavioral analysis on FPGA***
  - Localization to validation
  - Behavior validation
- ***Conclusion***

Counter case

- ***Static light emission*** *: Localization of the different function blocks*

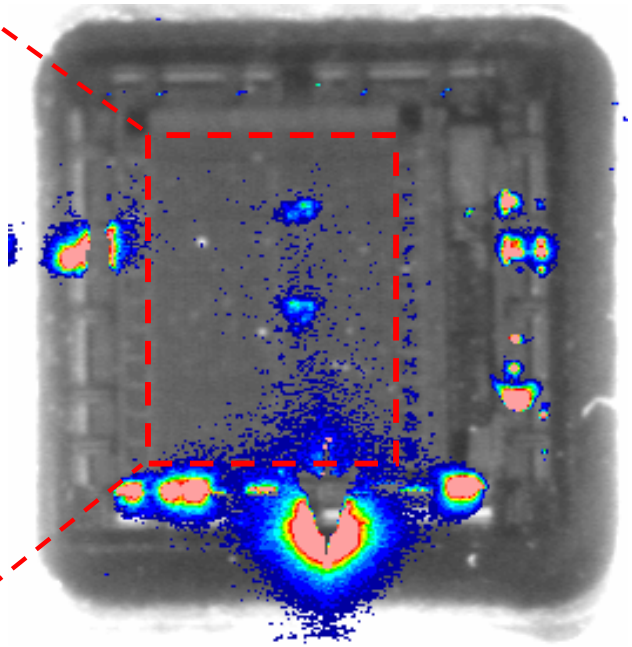


16 bits counter x 2



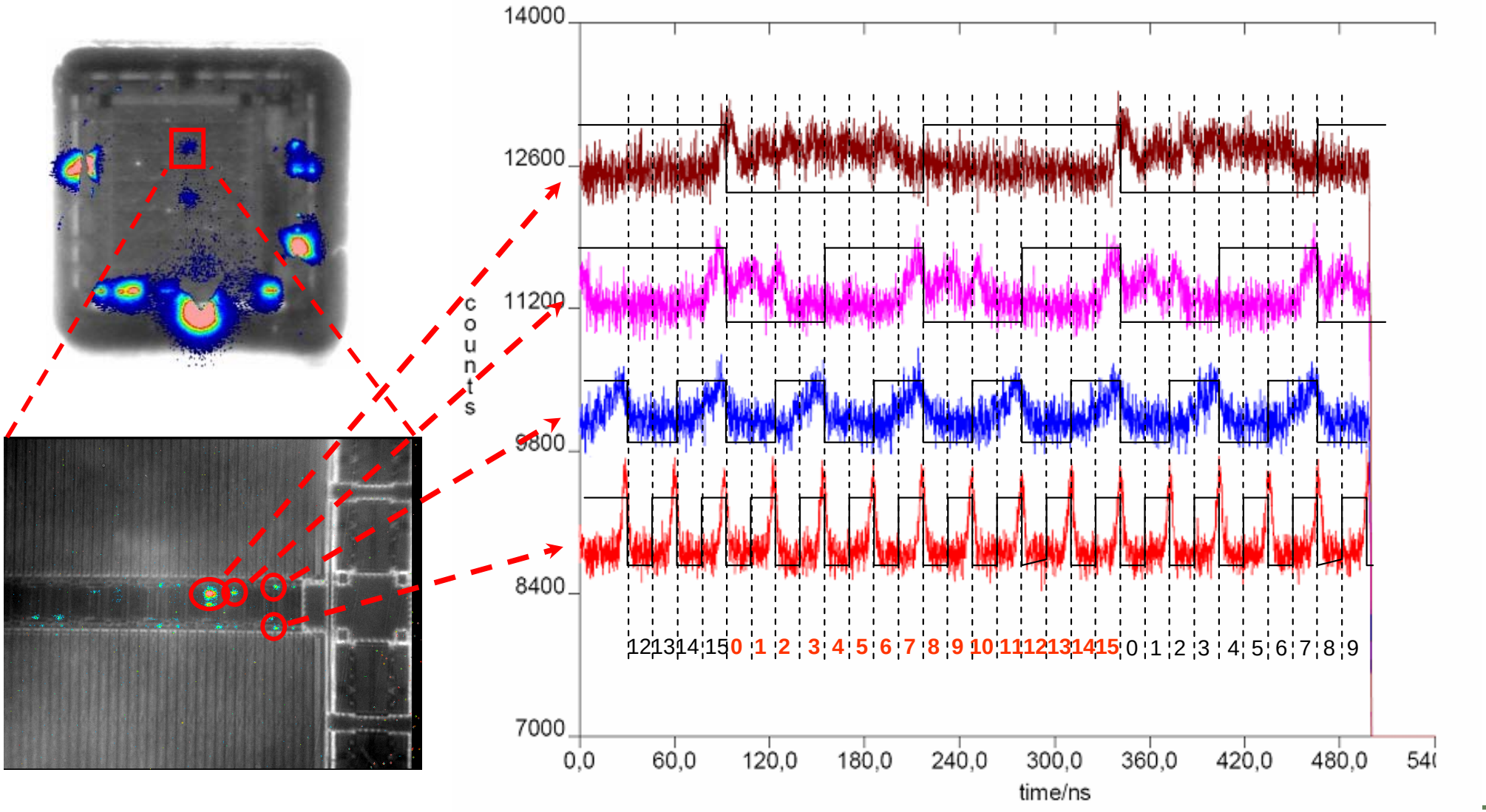
Software Design :

VHDL > Simulation > Implémentation



Emission Mapping [0.5x]

- Dynamic Light Emission : *Use of PMT (Photo Multiplier Tube) to validate the correct counter behavior*



Different approach :

- PICA data post processing **: Vectorizing and comparing**
- Dynamic mapping decomposition **: Extracting visual data**
- PMT behavioral analysis **: Extracting chronogram**

Drawbacks :

- **Not sufficient for a complete analysis**
- **Most efficiency if these methods are combined with a partial reverse of the circuit**
- **Needs physical access to the chip by non trivial IC preparation (back side thinning)**

- Thank you for your attention
- Questions?

Contact **:**

Jerome.dibattista@thales-is.cnes.fr