Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier
LIRMM

THALES

cnes

Light Emission Analysis on FPGA :
a new side channel possibility

Jérôme Di-Battista (Thales), Bruno Rouzeyre (LIRMM), Lionel Torres (LIRMM), Jean-Christophe Courrege (Thales), Perdu Philippe (CNES)

CNES & THALES

➢ *Partnership CNES / Thales (1990) :*

Common laboratory :

- **Expertise laboratory** (*CNES*)
- **Failure analysis activity** (Thales - *CEL*)
- **Security evaluation CESTI** (Thales - *CEACI*)

➢ *Introduction*

- Purpose
- Light Emission overview
- Last year results

➢ *Dynamic Light Emission*

- Dynamic Technique overview
- Behavioral Analysis on FPGA

➢ *New Side Channel Possibility*

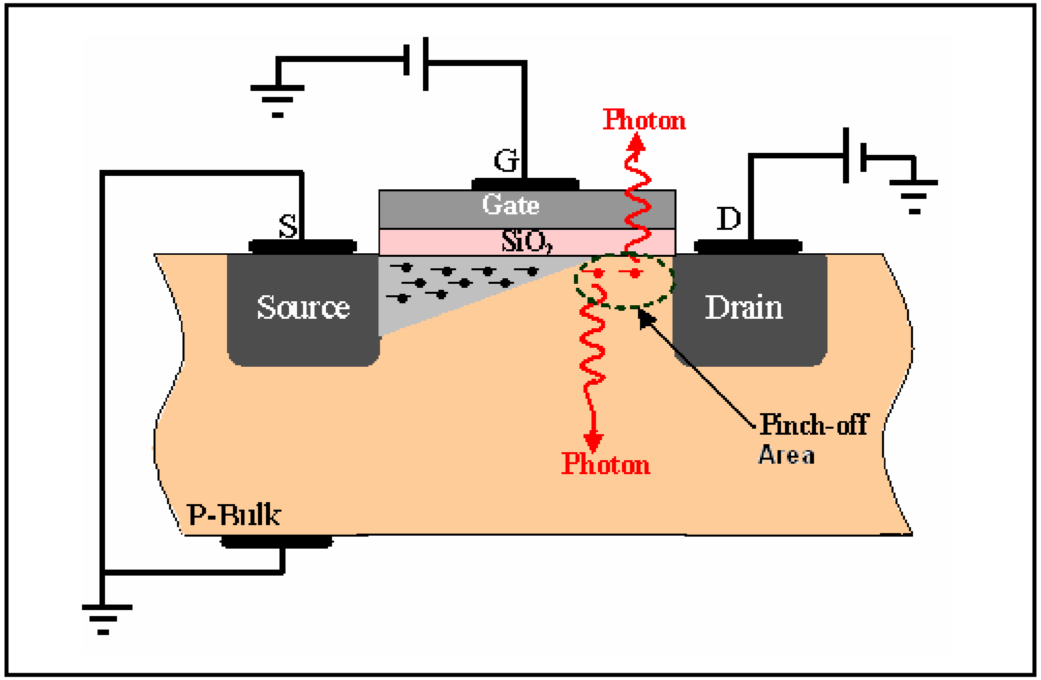
- DLEA: Differential Light Emission Analysis
- First results

Purpose

- **Use of failure analysis tools for security evaluation**
- **Explore light emission as a side-channel information**
- **Develop a methodology to perform a DPA-like attack based on dynamic light emission**

Light Emission (1/3)

nMOS transistor

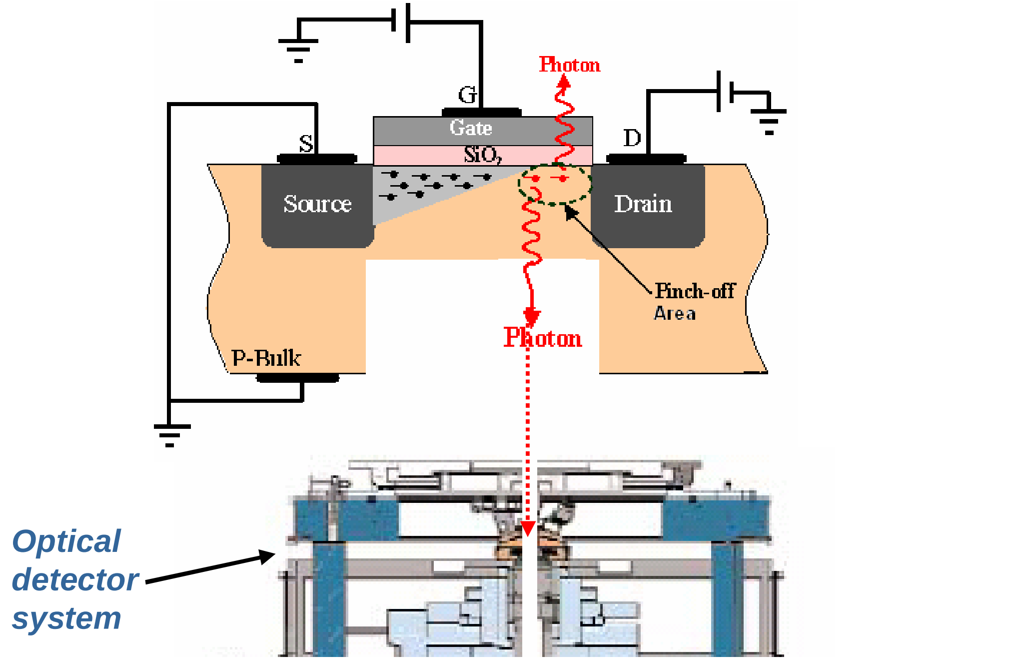


Radiative "desexcitation" of the charger carriers in **pinch-off area**, created a photon visible in **near-infrared** spectral range.

- **Light emission quality** :
  - **Frontside** : Depends on the number of metal layer (actually useless).
  - **Backside** : Need to thin down the silicium substract but .

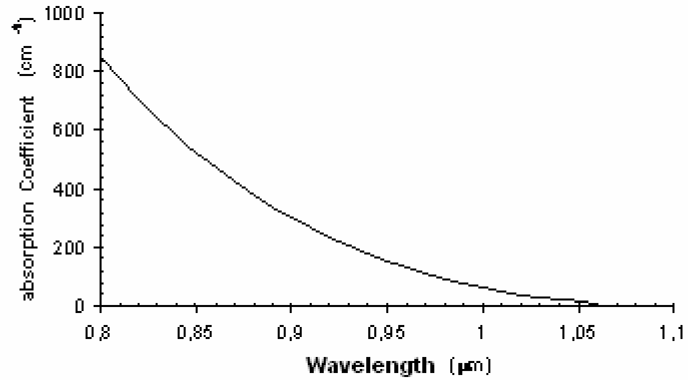
Light Emission (2/3)

nMOS transistor



Photon emission depends on:

V_{GS}, I_{DS}, V_{DS} & transistor size

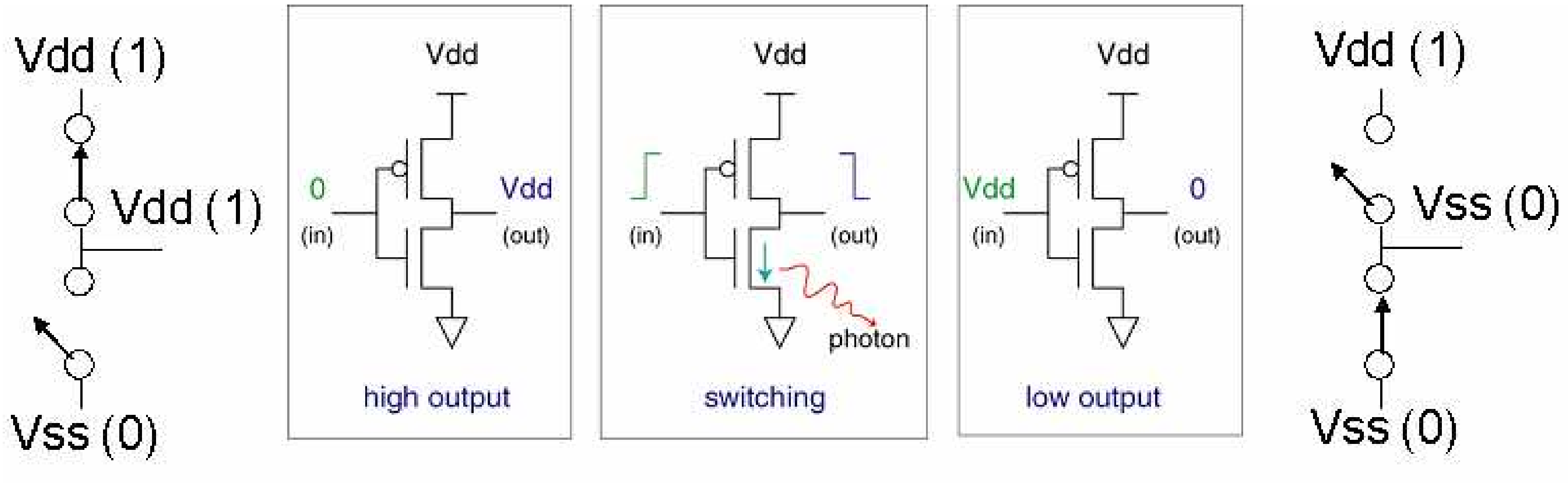


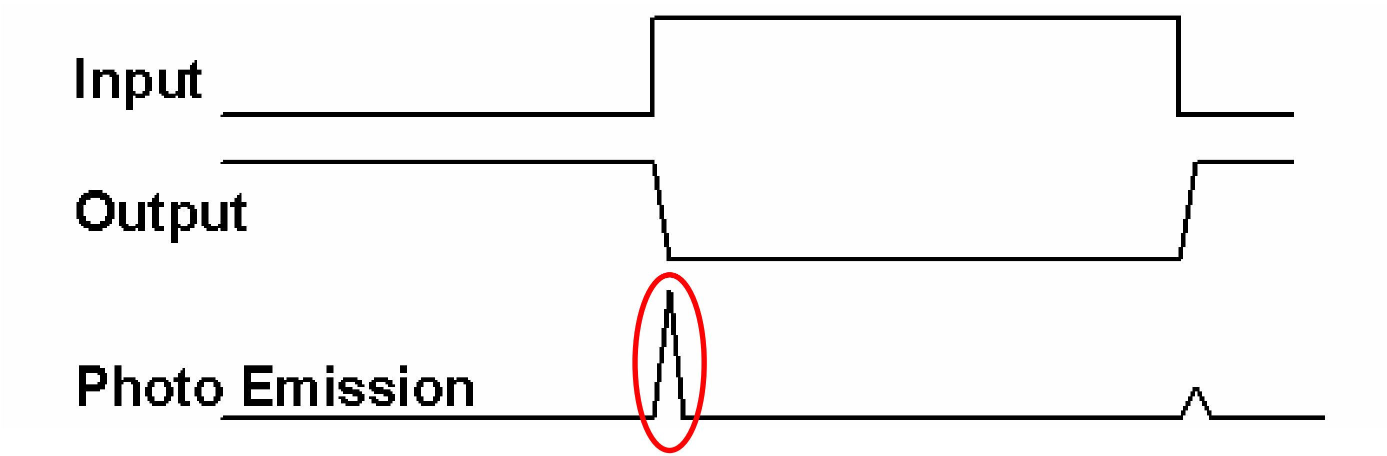
Absorption coefficient of silicium in function of optical beam wavelength

detector system
- ✓**CCD silicium captor wavelength: λ = 400 – 1200 nm**
  or
- ✓**InGaAs captor wavelength: λ = 900 – 1500 nm**

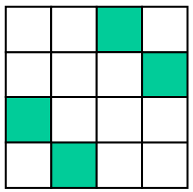
Infrared : λ = 780nm – 100 µm
Visible : λ = 400 – 745 nm

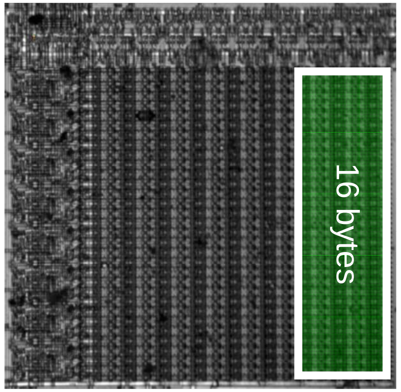
Light Emission (3/3)



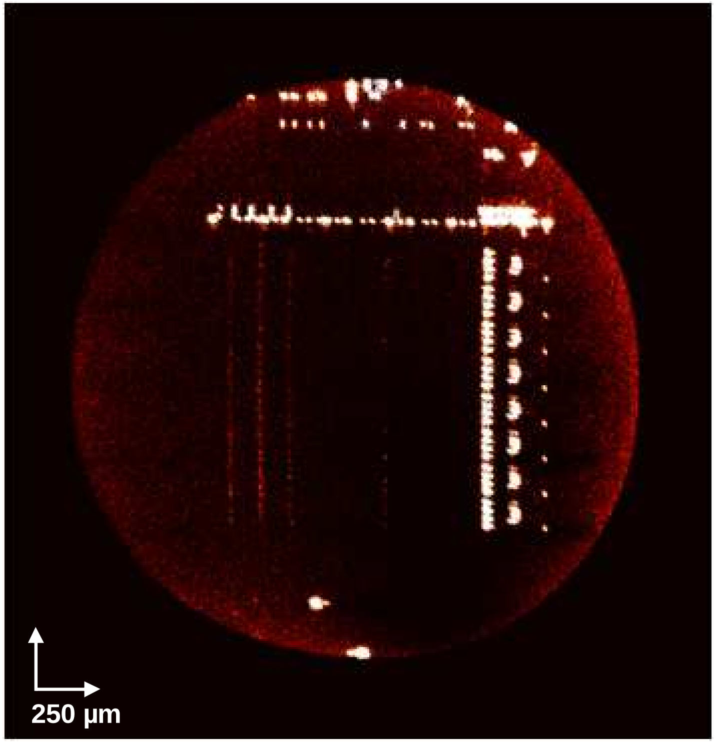


Last year results (1/3)





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



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

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

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

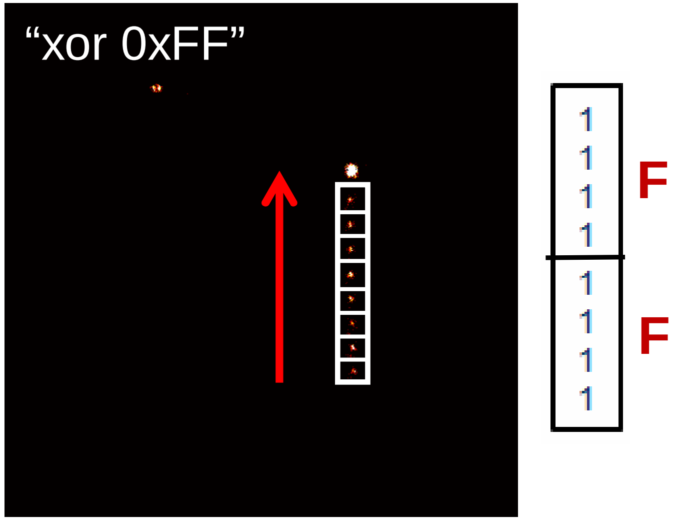
byte stays => just noise

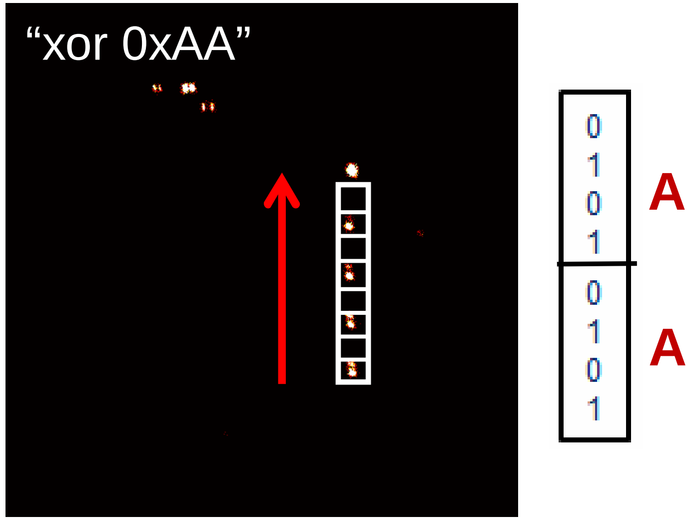
Last year results (2/3)

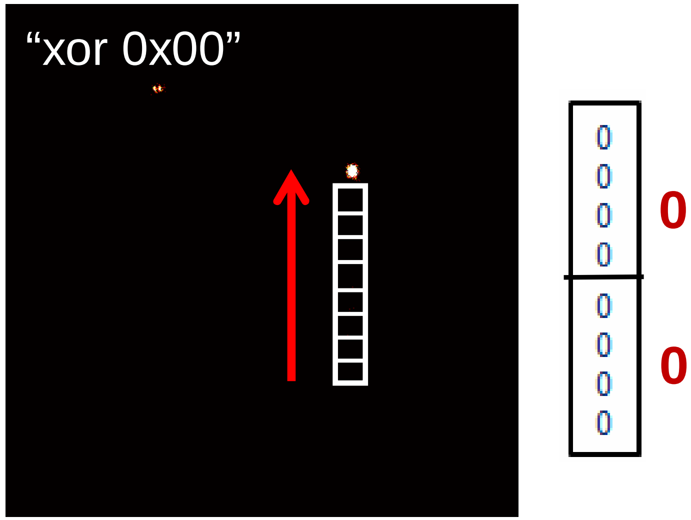
1 frame = 166 ns

Last year results (3/3)

3rd clock reveal the key







Martin Hlaváč, Julie Ferrigno, When AES blinks : introducing optical side-channel IET Information Security -- September 2008 -- Volume 2, Issue 3, p. 94-98

➢ *Introduction*

- Purpose
- Light Emission overview
- Last year result

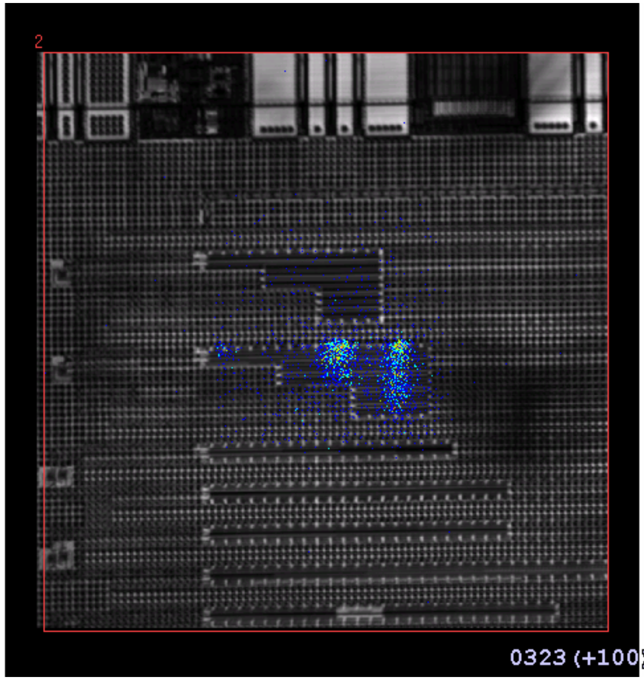
➢ *Dynamic Light Emission*

- Dynamic Technique overview
- Behavioral Analysis on FPGA

➢ *New Side Channel Possibility*

- DLEA: Differential Light Emission Analysis
- First results

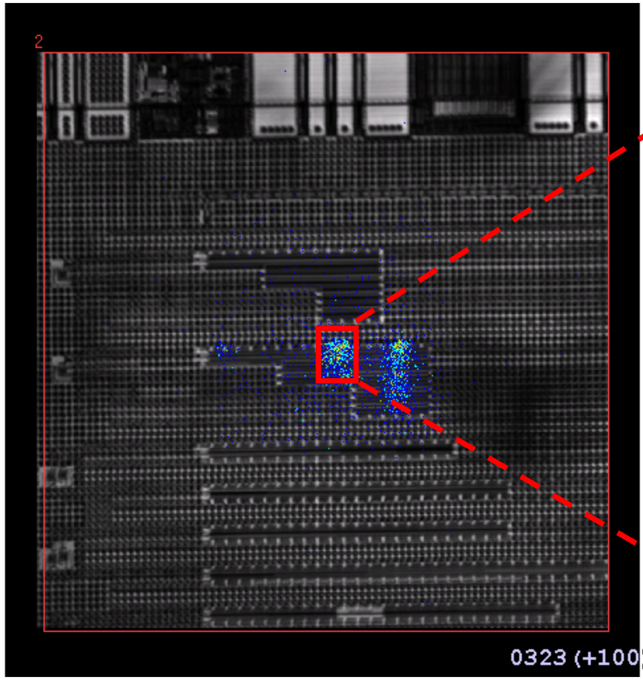
Dynamic Light emission (PICA)

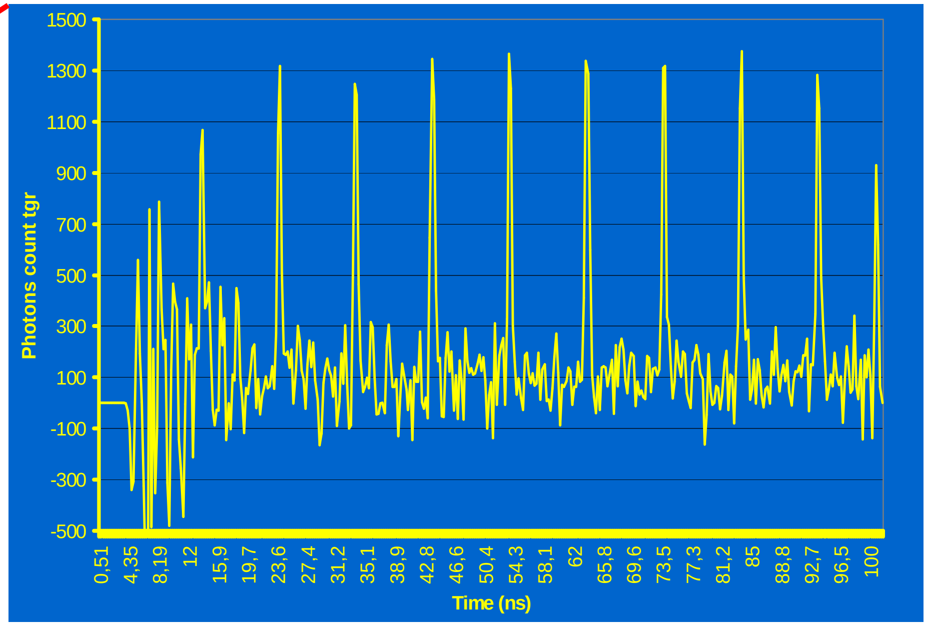


PICA (Picosecond Imaging circuit analysis)

- **Saturation occurs briefly during commutation**
- **Electrical signal propagation path**
- **Direct probing of sensitive data**

Dynamic Light emission (PICA + TRE)





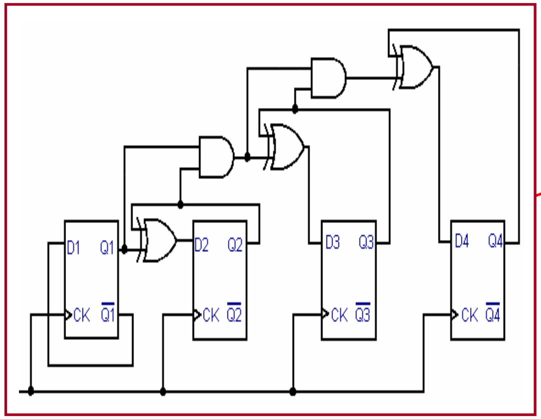
PICA (Picosecond Imaging circuit analysis)

TRE curves (Time Resolved Emission)

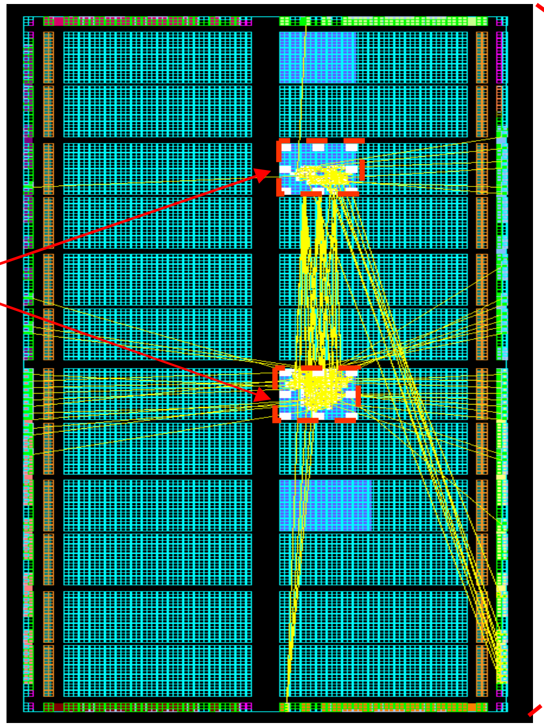
- Saturation occurs briefly during commutation
- Electrical signal propagation path
- Direct probing of sensitive data

Behavioral analysis (1/2)

- The goal is to determine the behavior of the function thanks to light emission
- Implementation of two 16 bits counters on FPGA proasic3E (Actel)

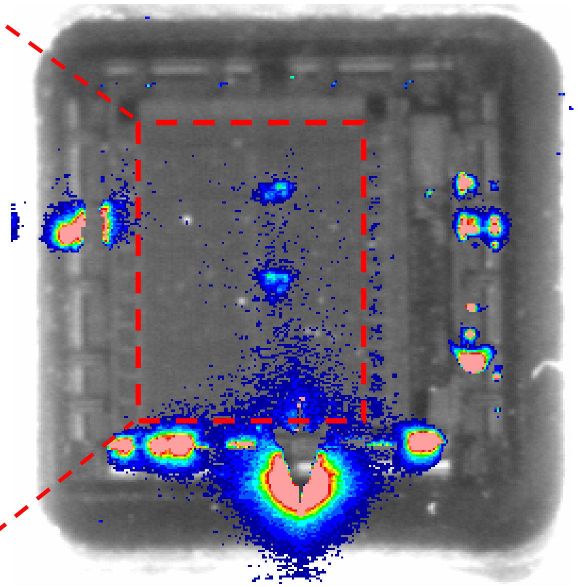


16 bits synchronous counter



Software Design :

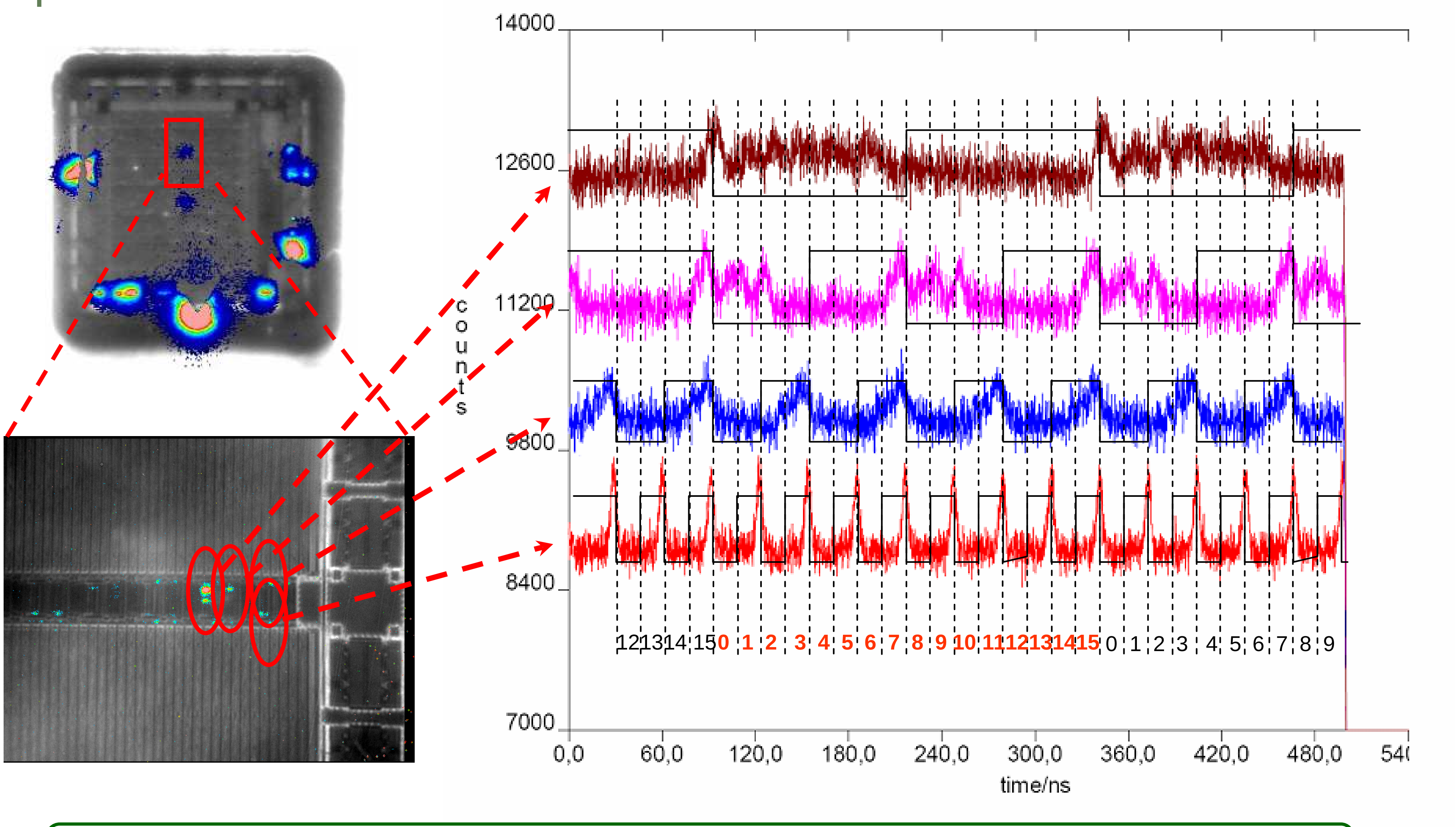
VHDL > Simulation > Implémentation



Emission Mapping [0.5x]

Static light emission: Localize the different function blocks

Behavioral analysis (2/2)



Dynamic Light Emission: to validate the internal behavior

➢ *Introduction*

- Purpose
- Light Emission overview
- Last year result

➢ *Dynamic Light Emission*

- Dynamic Technique overview
- Behavioral Analysis on FPGA

➢ *New Side Channel Possibility*

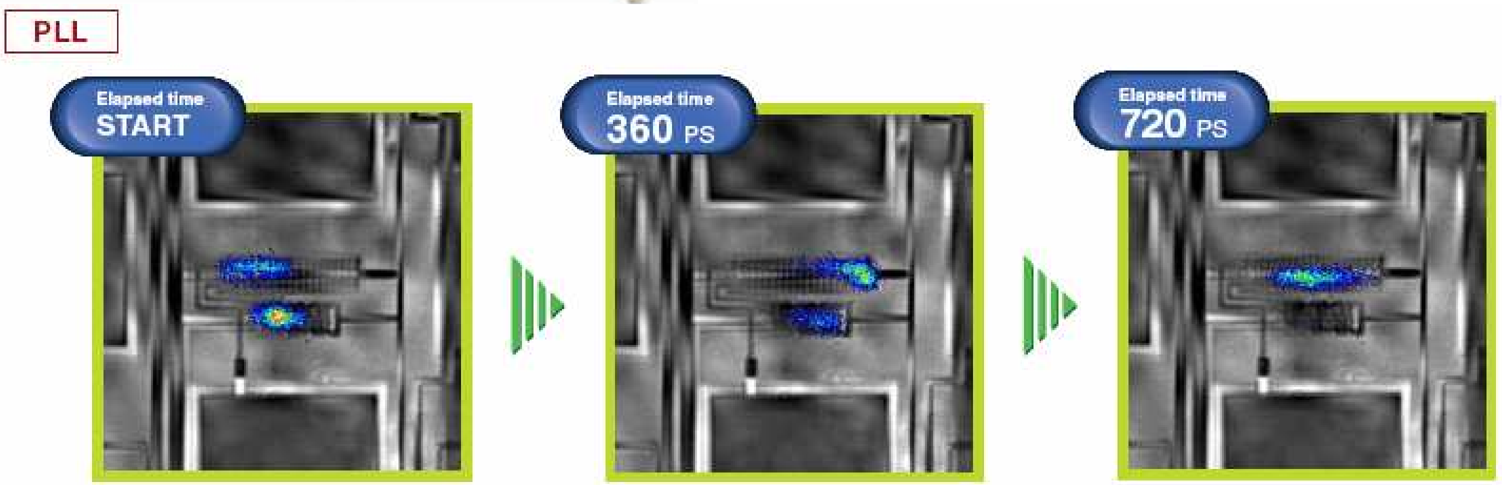
- DLEA: Differential Light Emission Analysis
- First results

Hamamatsu Tri-PHEMOS

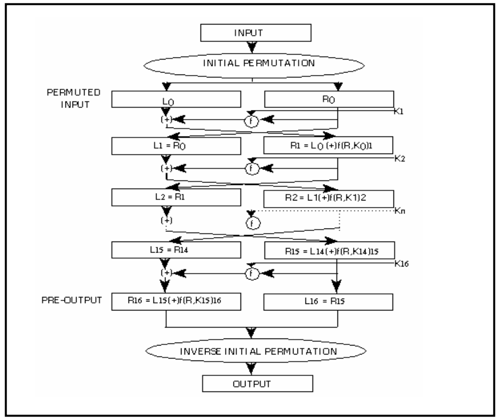
➢ ***3 camera types:***
InGaAs / InSb / CCD camera

➢ ***Objective lens:*** *1x / 2.5x / 20x / 100x*

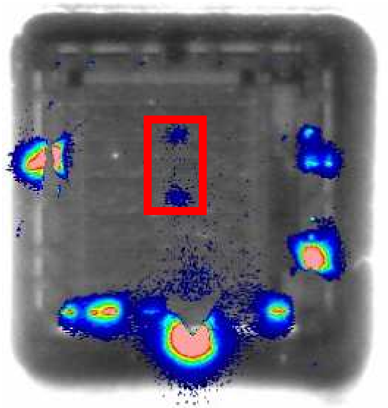
➢ ***Laser selection :*** *1.3 µm Laser (100 mW)* ***/*** *1.3 µm High Power laser (400 mW)* ***/*** *1.1 µm Pulse Laser (200 mW)*



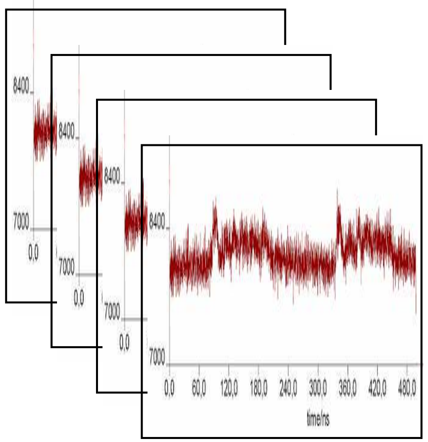
DLEA => Differential Light Emission Analysis :



Cipher algorithm implementation



DES Localisation



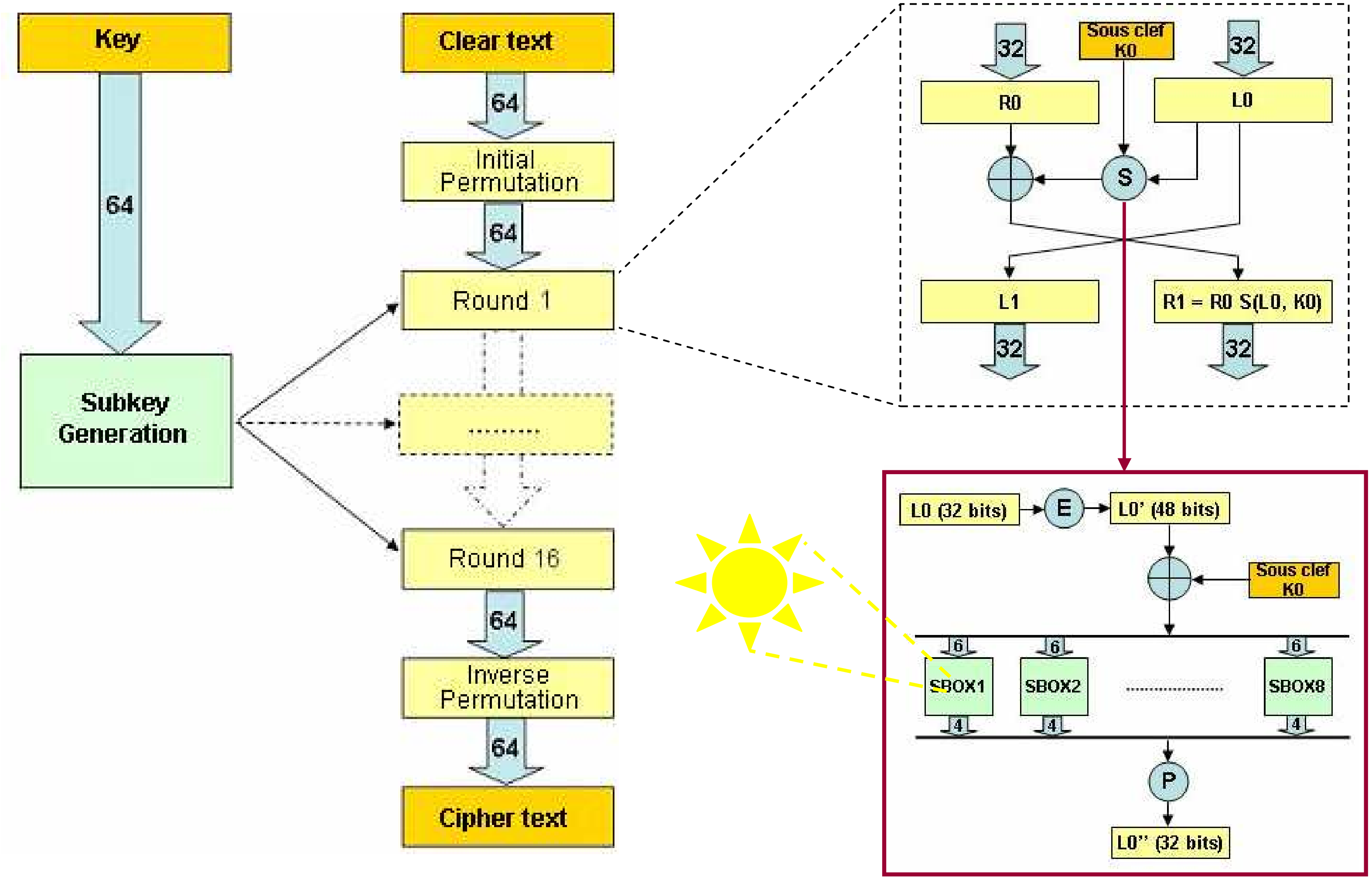
TRE curves

Mesuring light emission during device operation :

- Variation of input data = time and spatial variation :
  - Differences between TRE curves
- Correlation between TRE curves and the Key used:

TRE curves (DLEA) ~ Power consumption curves (DPA)

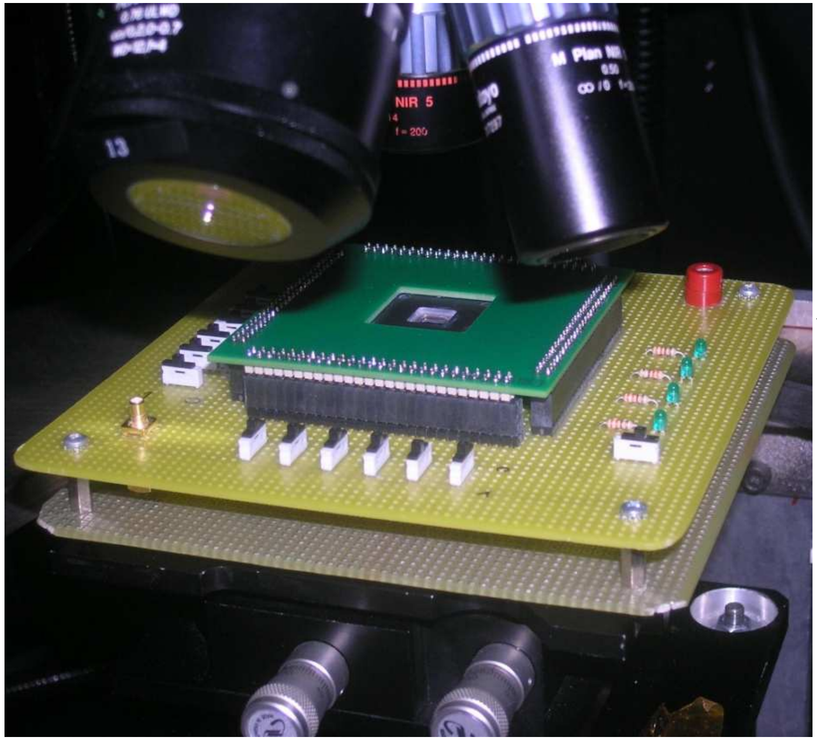
Target of attack

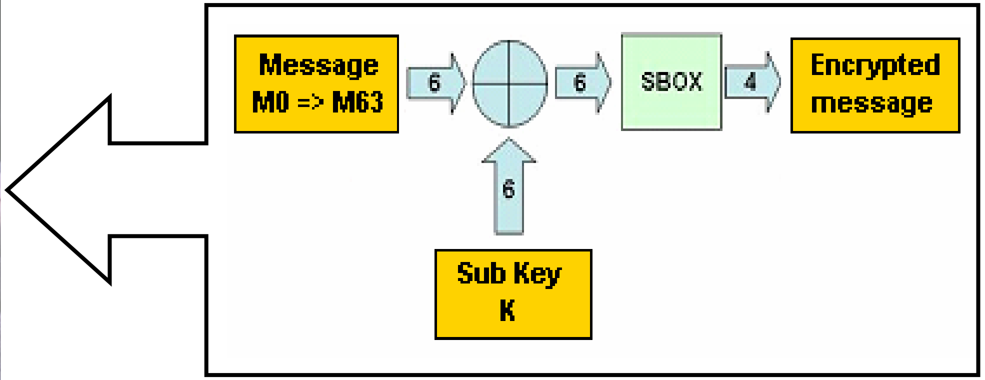


Attack on 1st SBOX of the 1st round of DES algorithm

Experimental setup

- Backside decapsulated FPGA Proasic3e on a test board



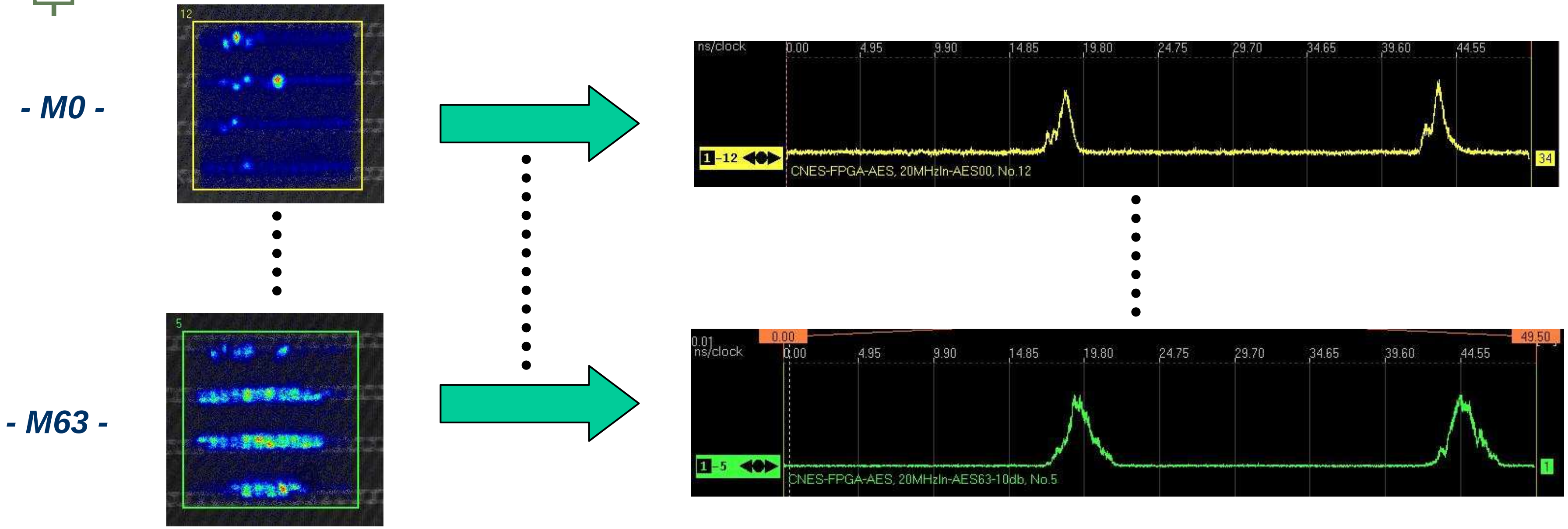


1st DES round implémentation on FPGA

- Experiment on a simple 1st DES round :

Message (0 to 63) **Xor** ***Subkey (26)*** **=>** SBOX **=>** Encrypted data

Acquisition process



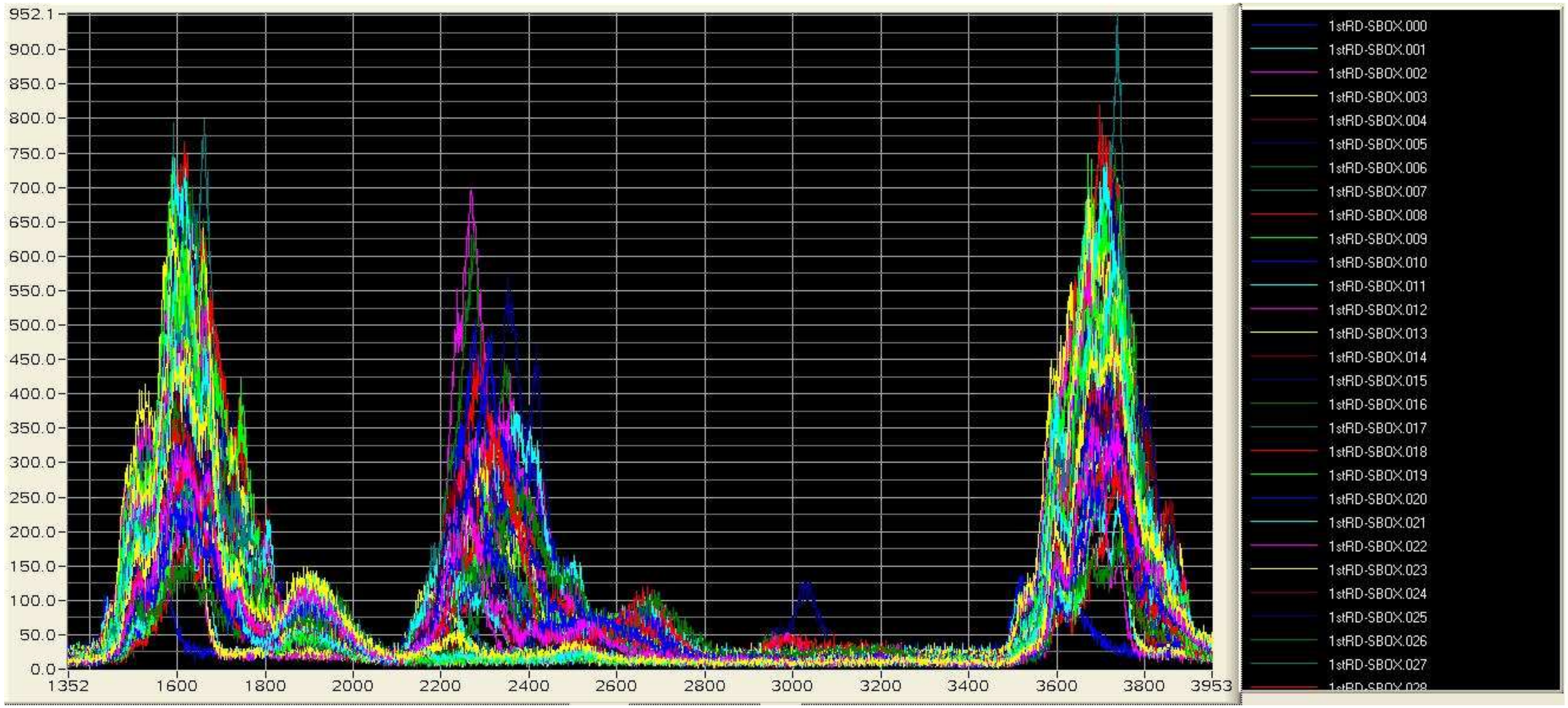
- The light emitted during 1 cycle clock are insufficient to be operated
- Single shot acquisition system:

Camera ON **[*Mx 00 Mx 00 Mx 00............Mx 00*]** **Camera OFF**

Counting photons during 1 minute

- Acquisition of TRE curves for each input message: ***M1 to M63***

DPA Processing

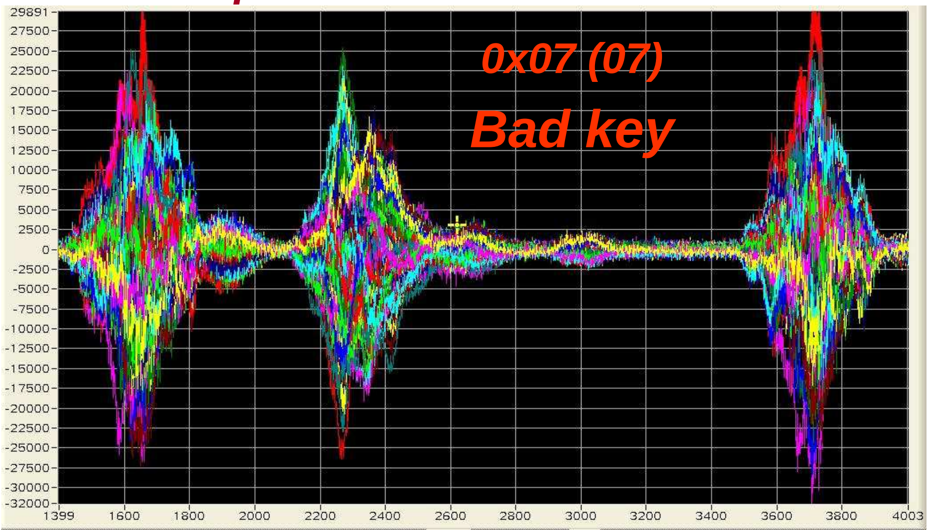


Acquisition process : [*Mx 00 Mx 00 Mx 00…........Mx 00]*

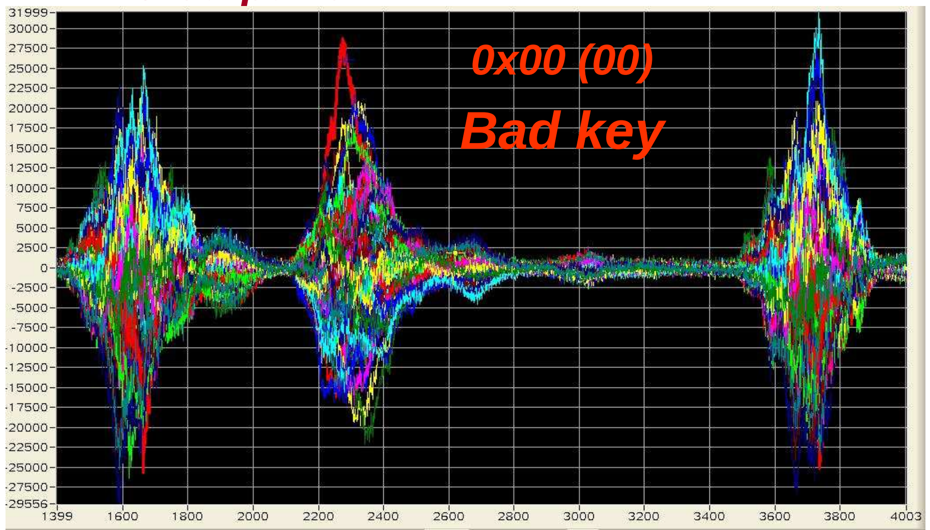
2 transitions : Mx => 00, 00 =>Mx ⟹ Hamming weight model

First Results 1/2

1st output bit

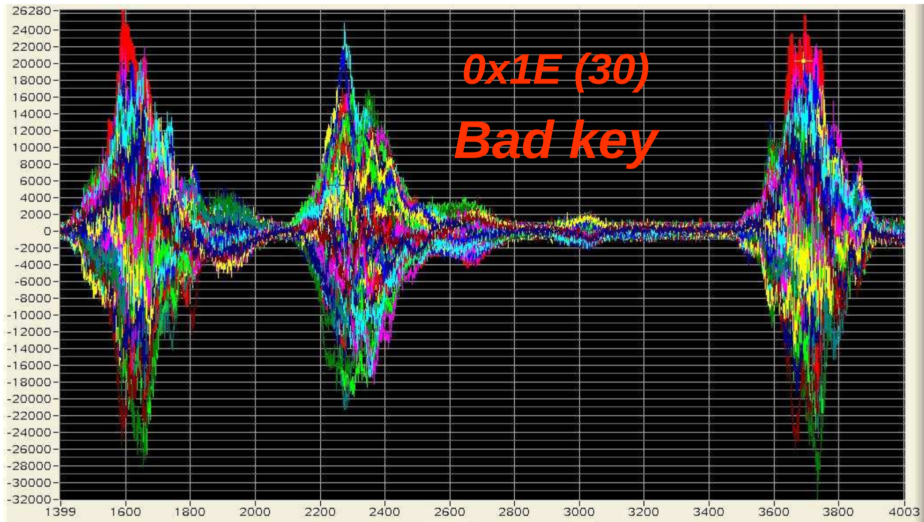


2nd output bit

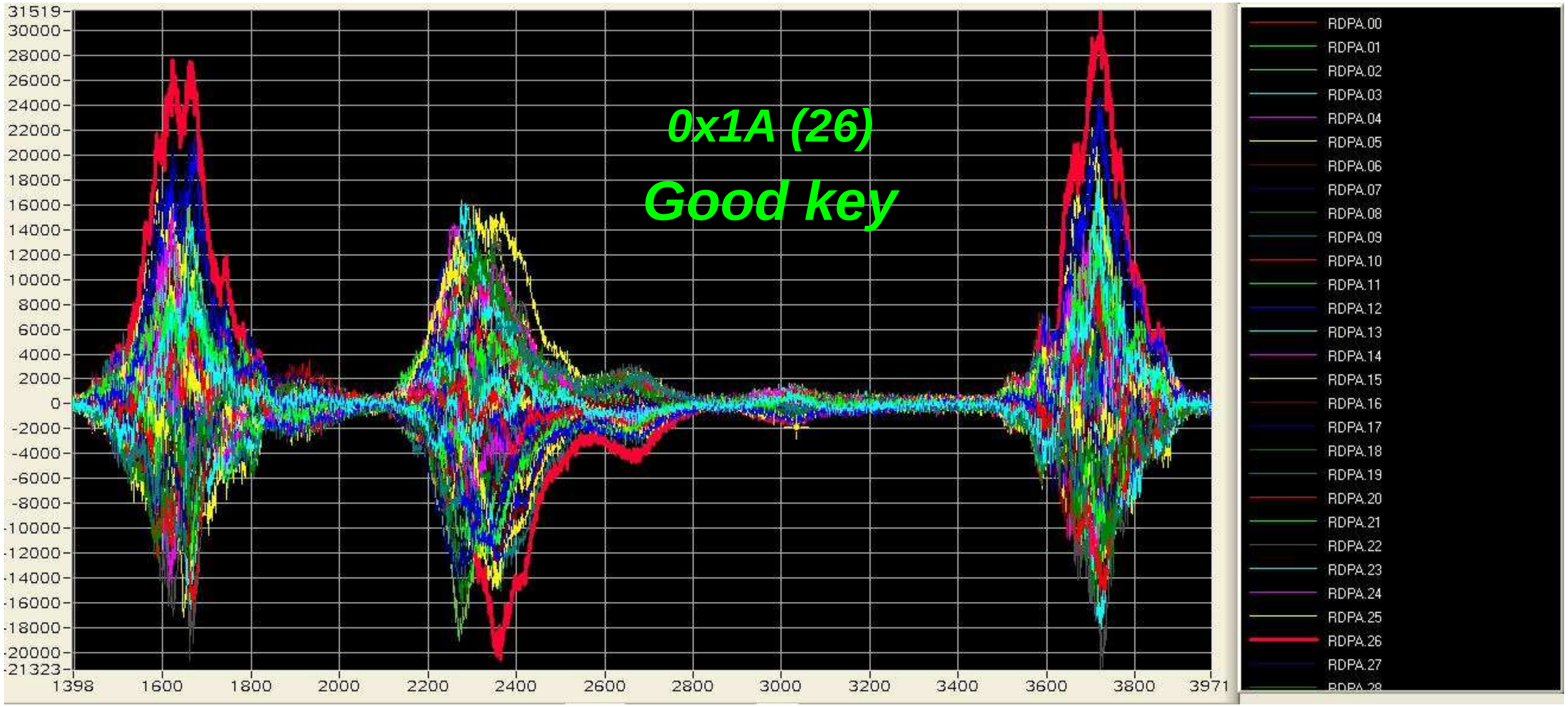


3rd output bit

4th output bit



First Results 2/2



Attack on the **3rd Bit** or **sum** of output bits reveal the good key

- In this case only time and photon counting datas was used, but spatial factor can bring a lot of complementary information for the attack.

Go into detail :

- **Compare the results with the other side channel attack to precisely specify the contribution of DLEA method.**
- **Efficiency of the attack by implementing the whole cipher algorithm.**
- **Effect of the different side channel countermeasures for this type of attack.**
- **Exploitation of the spatial information to improve the DLEA attack.**
- **Introduce specific countermeasures.**

Dynamic light emission :

- **It is possible to localize the different functions using static technique.**
- **It is possible to determine the behavior of function using dynamic technique (and partial knowledge of the design).**
- **With time information and photon counting, Differential Light Emission Analysis (DLEA) allows to extract the good key from 1st round of DES algorithm.**

Countermeasures and issues :

- **Latest technology (45 nm): The Spectral range shift induce an issue with light emission detector.**
- **On FPGA case, a Dynamic reconfiguration can change the light emission profile.**
- **Latest light emission equipment cost : ~ 2 M€ ☹**

- **Thank you for your attention**
- **Questions?**

Contact **:**

Jerome.dibattista@thales-is.cnes.fr