When Failure Analysis Meets Side-Channel Attacks

Jérôme DI-BATTISTA (THALES), Jean-Christophe COURREGE (THALES), Bruno ROUZEYRE (LIRMM), Lionel TORRES (LIRMM), Philippe PERDU (CNES)

Outline

➢ *Introduction*

- Context
- Failure analysis
- Test vehicle

➢ *Light Emission as a Side-Channel signal*

- Background
- Experimental setup
- Results

➢ *Laser to improve Side-Channel attacks*

- Background
- Experimental setup
- Results

Outline

➢ *Introduction*

- Context
- Failure analysis
- Test vehicle

➢ *Light Emission as a Side-Channel signal*

- Background
- Experimental setup
- Results

➢ *Laser to improve Side-Channel attacks*

- Background
- Experimental setup
- Results

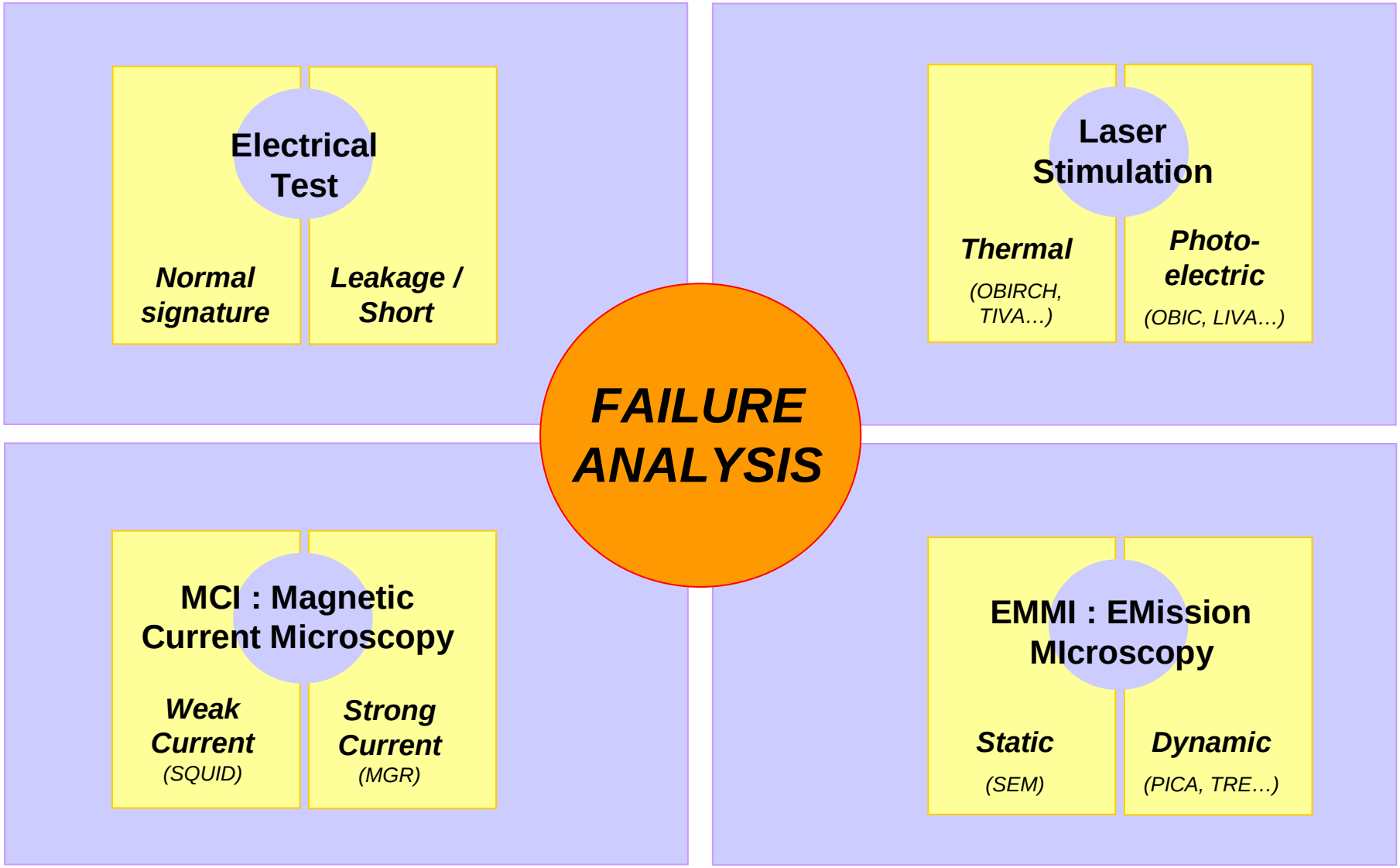
cnes & THALES

➢ *Partnership CNES / Thales :*

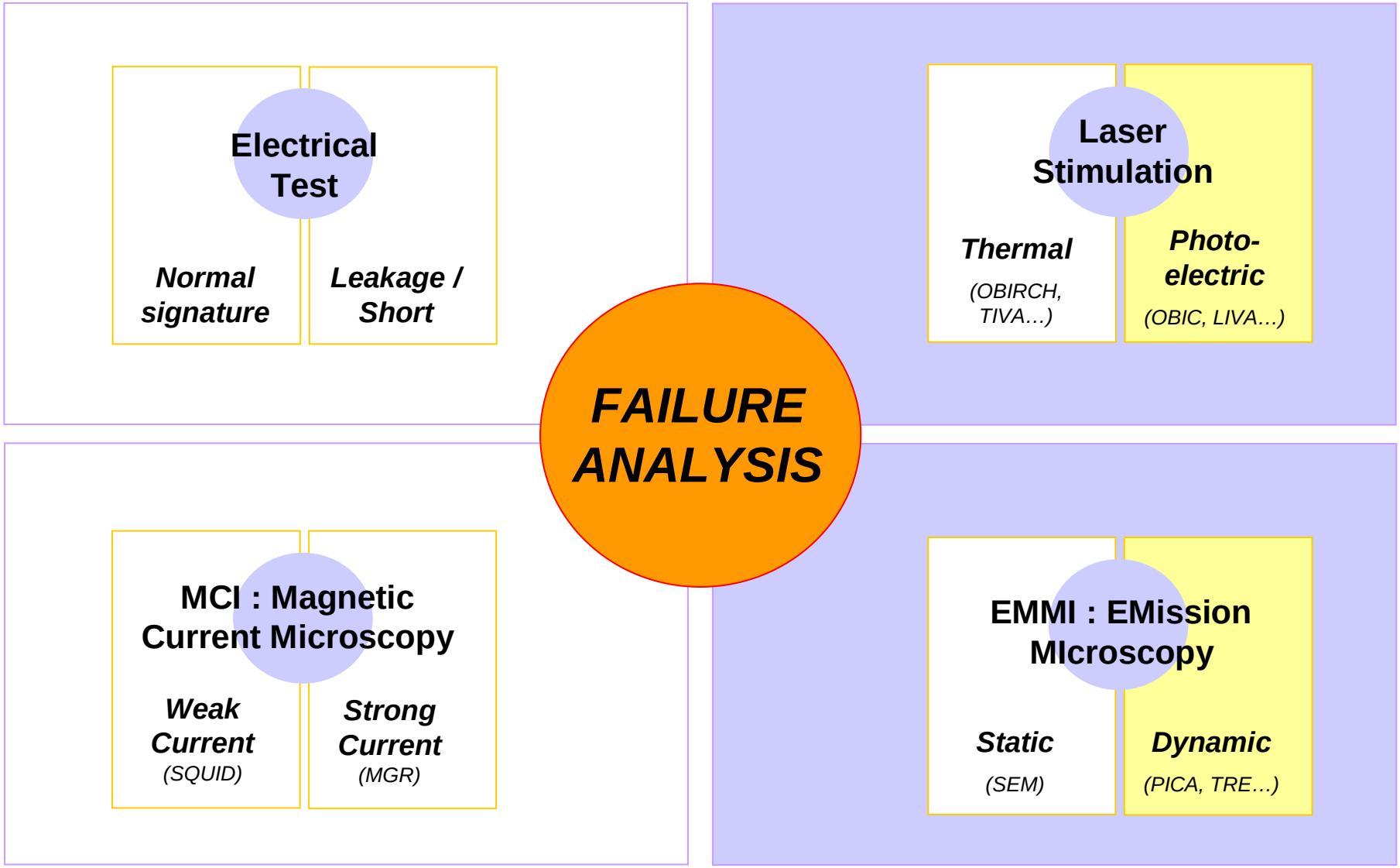
Common laboratory :

- **Failure analysis activity** (*CNES*)
- **Security evaluation ITSEF** (Thales - *CEACI*)
- **Electrical and physical testing** (Thales - *CEL*)

Failure analysis overview

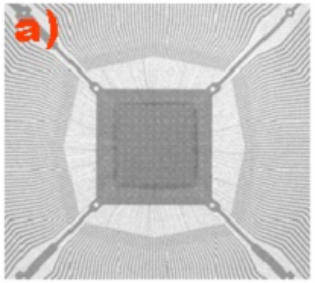


Failure analysis overview

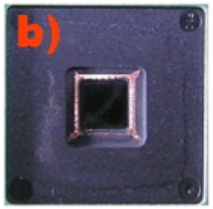


FPGA sample

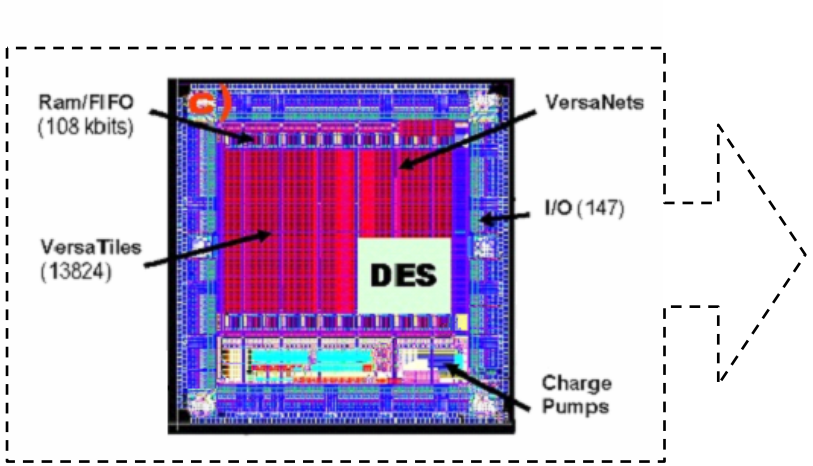
- Different view and informations about the **FPGA Actel® Proasic3e** :



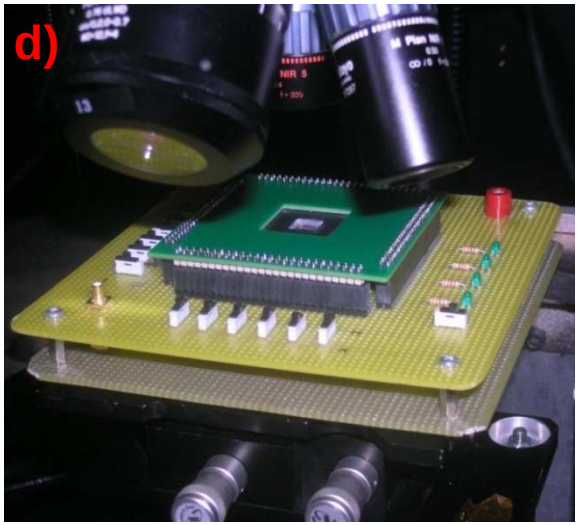
X-ray image



Backside aperture



Layout informations / location of DES implementation



FPGA test board

- **Light Emission** : Experiment on the 1st DES round :

64 Messages **Xor** ***random Subkey*** **=>** SBOX **=>** Encrypted data

- **Laser stimulation** : Experiment on a full DES :

16000 Messages & ***random key*** **=>** DES **=>** Encrypted data

Outline

➢ *Introduction*

- Context
- Failure analysis
- Test vehicle

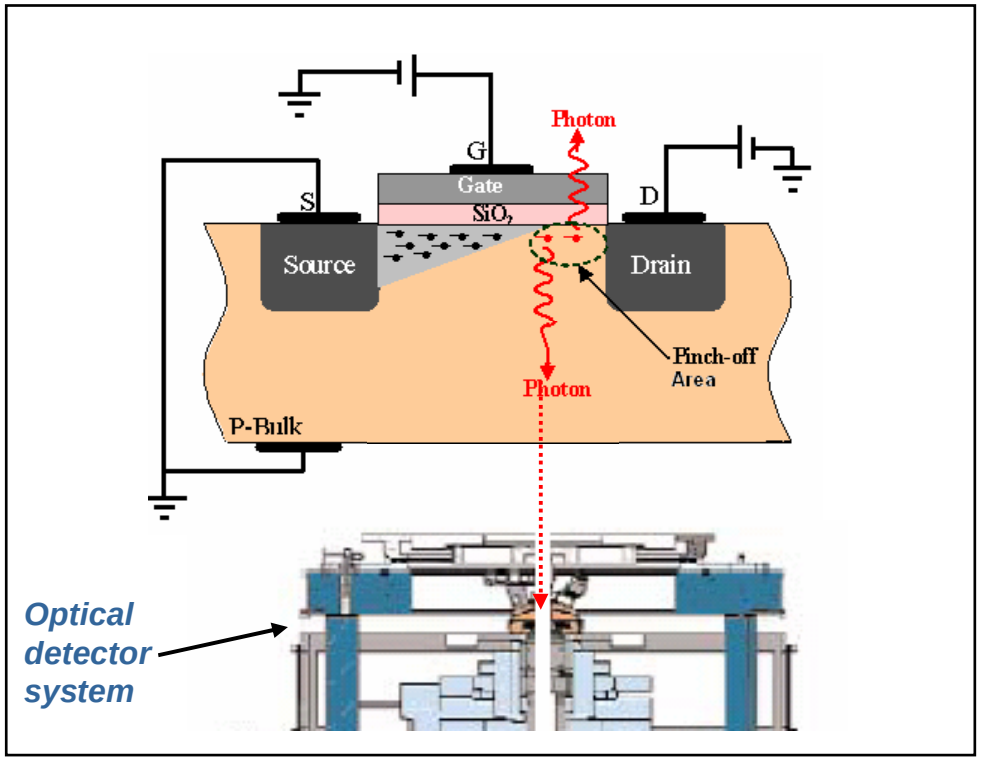
➢ *Light Emission as a Side-Channel signal*

- Background
- Experimental setup
- Results

➢ *Laser to improve Side-Channel attacks*

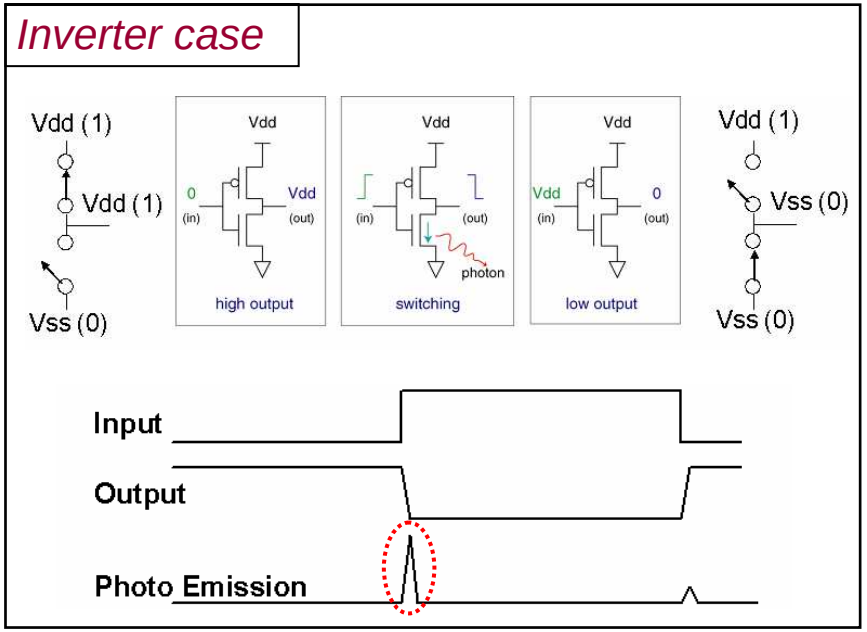
- Background
- Experimental setup
- Results

nMOS transistor



Photon emission depends on:

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

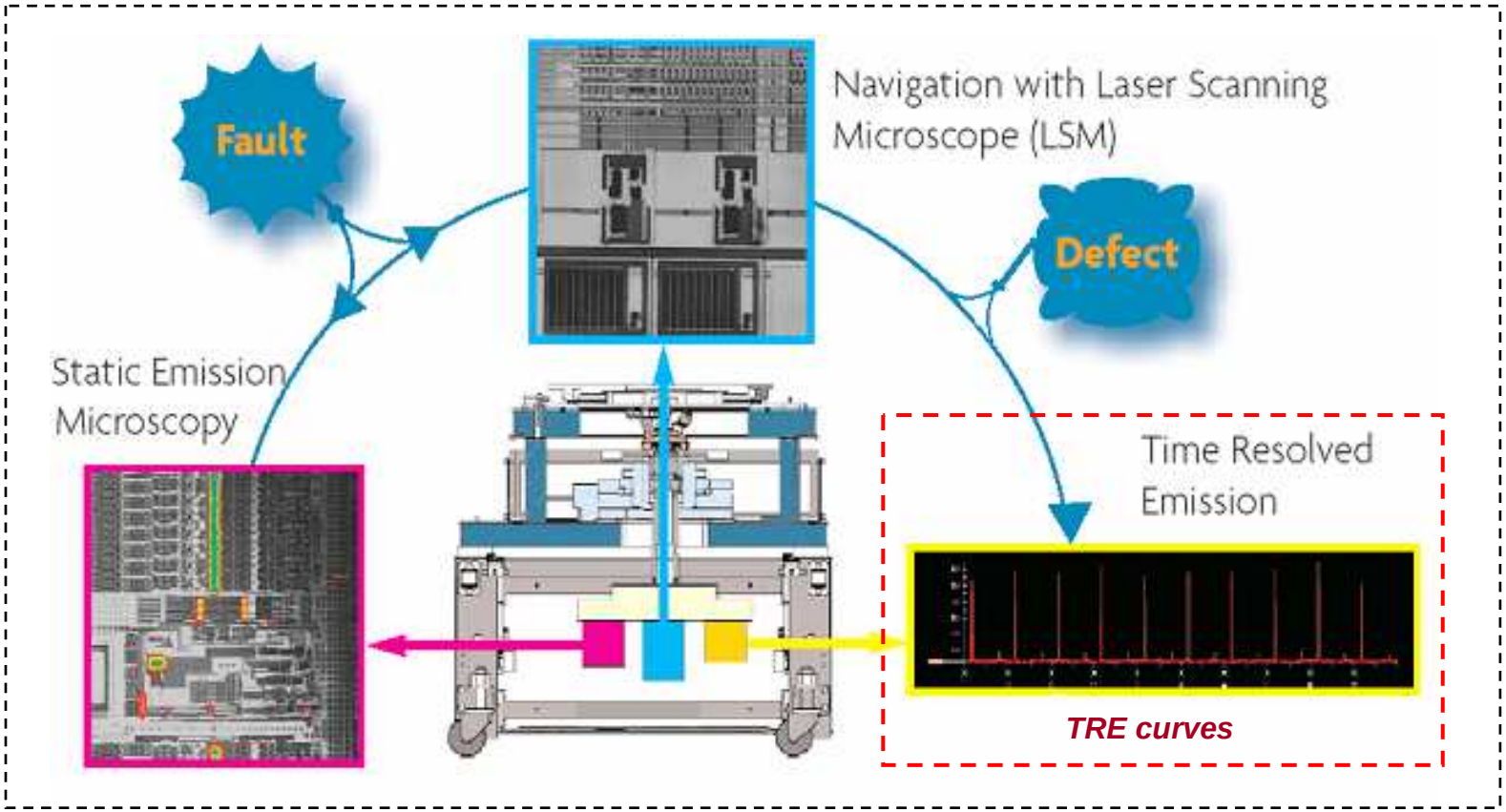


detector system

- ✓ **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

TRE Dynamic technique



- Many techniques were developed in failure analysis using EMMI:
  - Static Emission Microscopy (SEM) : spatial coordinate (x,y)
  - **Dynamic Emission Microscopy (TRE, PICA) : time information**

Hamamatsu Tri-PHEMOS

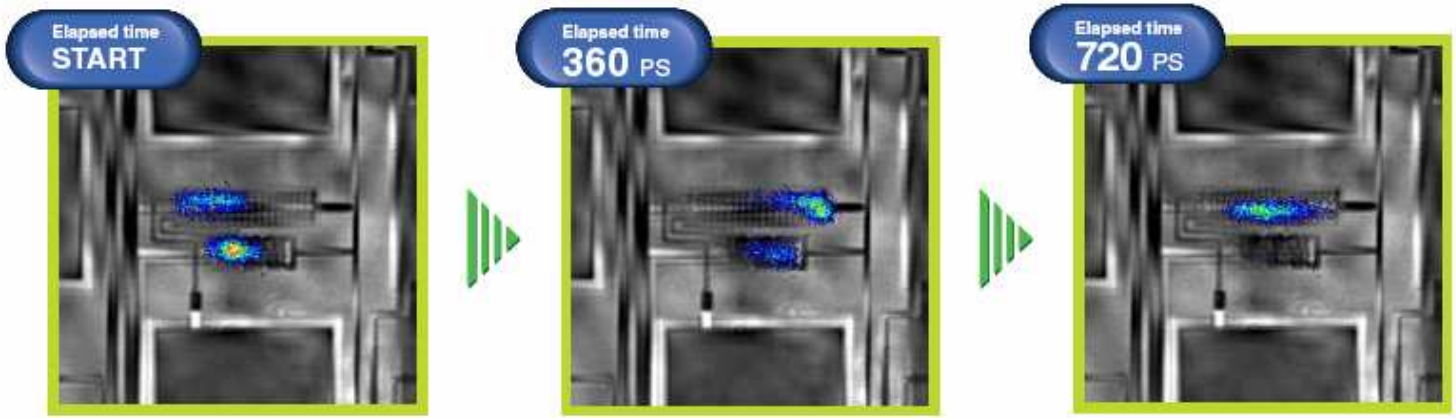
- ***Camera types:***

  InGaAs *:* 950nm to 1400nm / 640x480 / pixel size of 20µm x 20µm

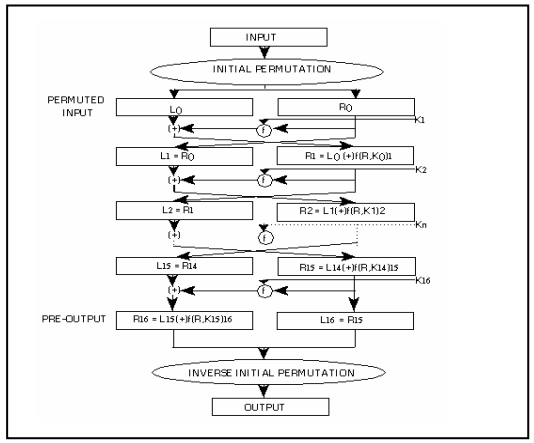
- ***Objective lens:*** *1x / 2.5x / 20x / 100x*

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

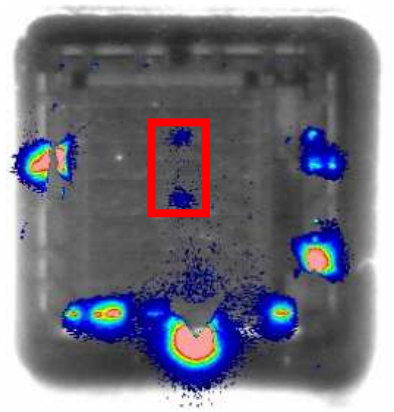
PLL



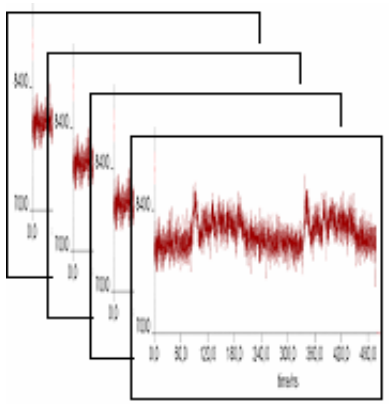
DLEA => Differential Light Emission Analysis :



Cipher algorithm implementation



SBOX Localisation



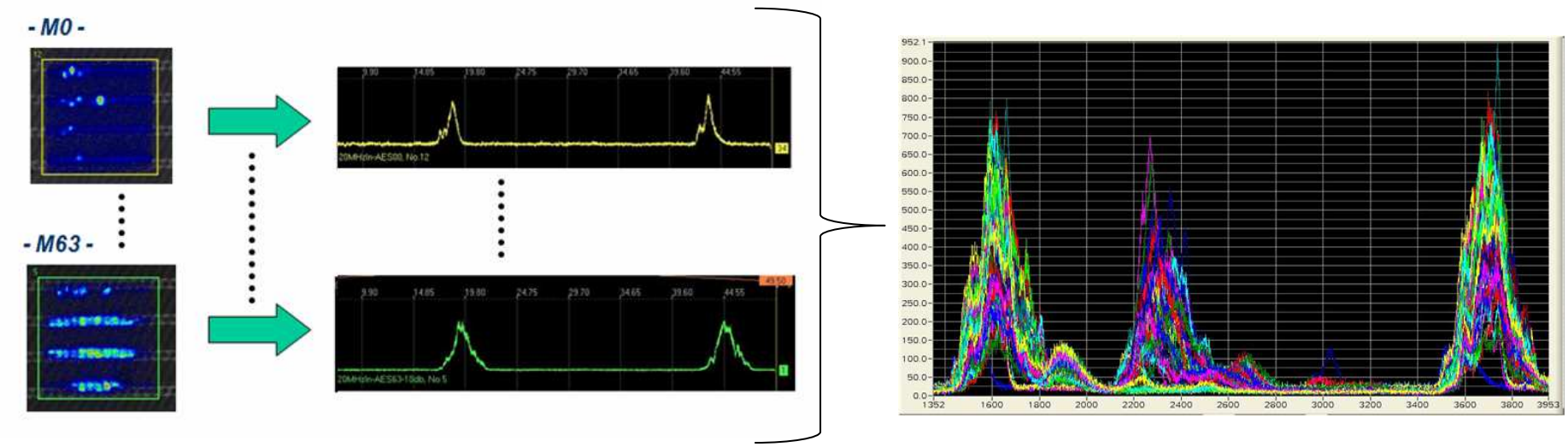
TRE curves

Mesuring light emission during device operation :

- Variation of plain text = time and space variation :
  - Differences between TRE curves
- Correlation between TRE curves and the Key used:

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

Process



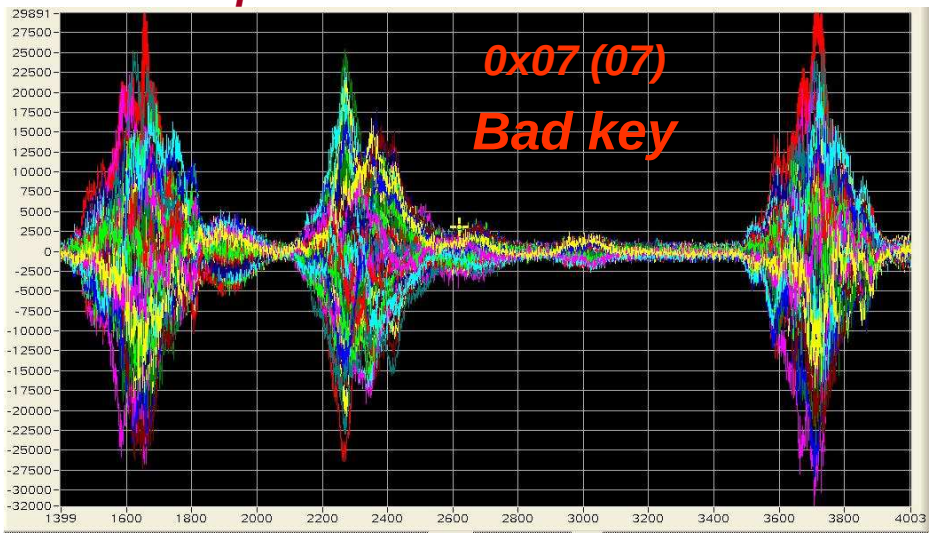
- The photons emitted during 1 cycle clock are insufficient to be operated
- Acquisition system:

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

Photons Counting during 20 seconds

- 2 transitions : 0 => 0 or 0 => 1 → **Hamming weight model**

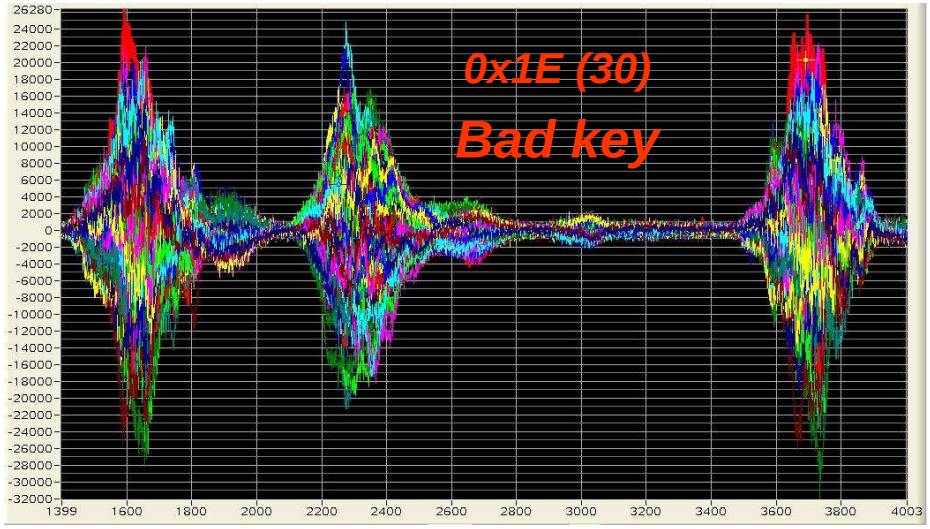
1st output bit



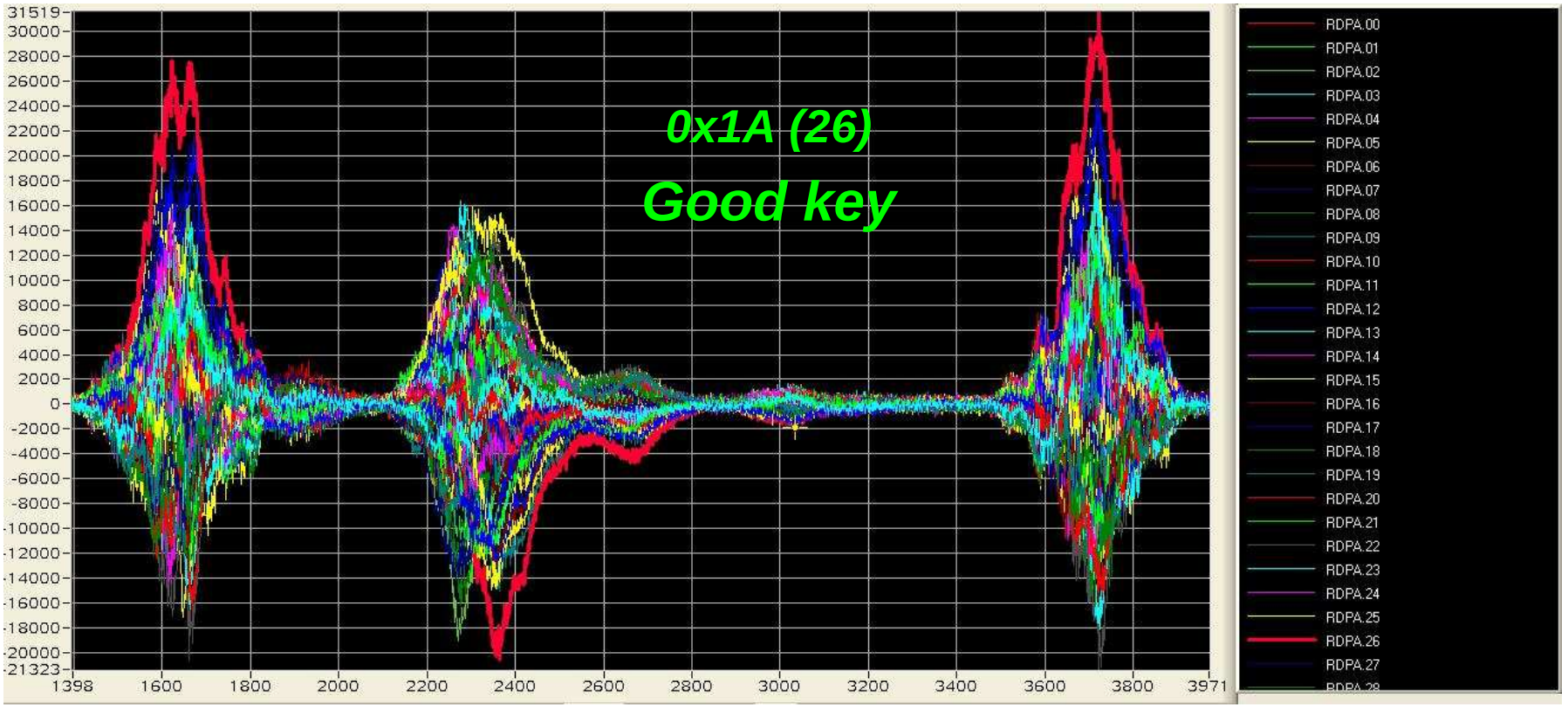
2nd output bit

3rd output bit

4th output bit



Results



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

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

Outline

➢ *Introduction*

- Context
- Failure analysis
- Test vehicle

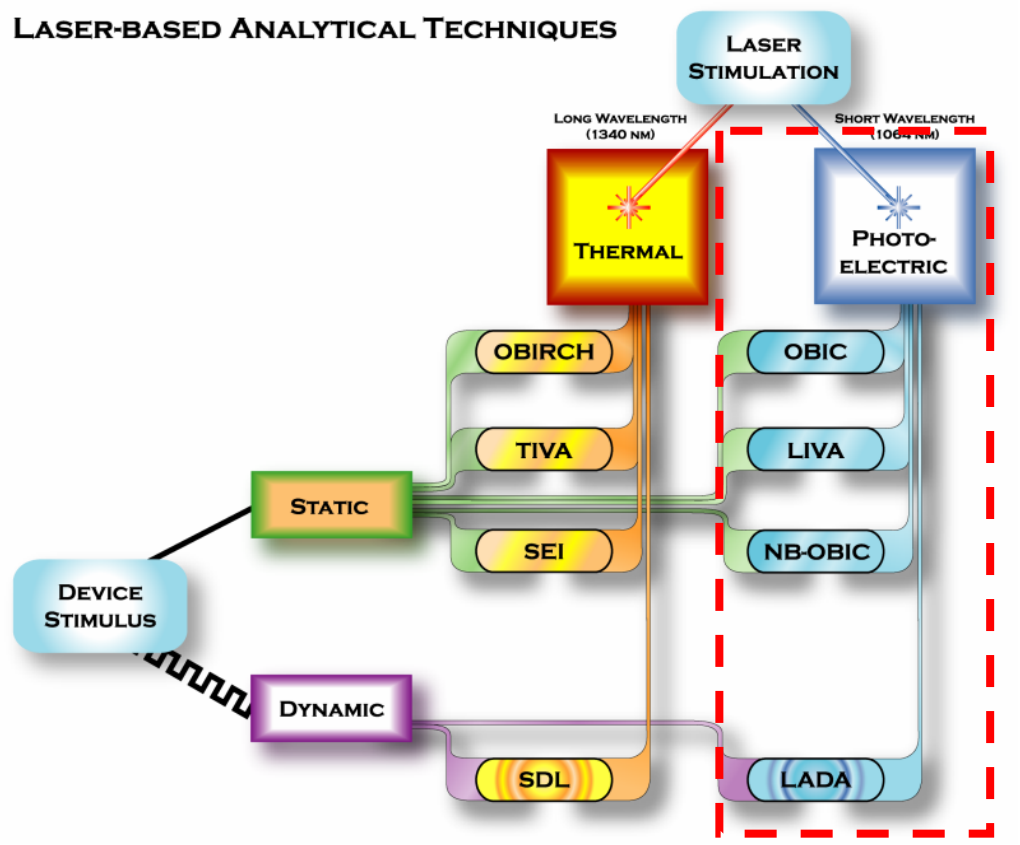
➢ *Light Emission as a Side-Channel signal*

- Background
- Experimental setup
- Results

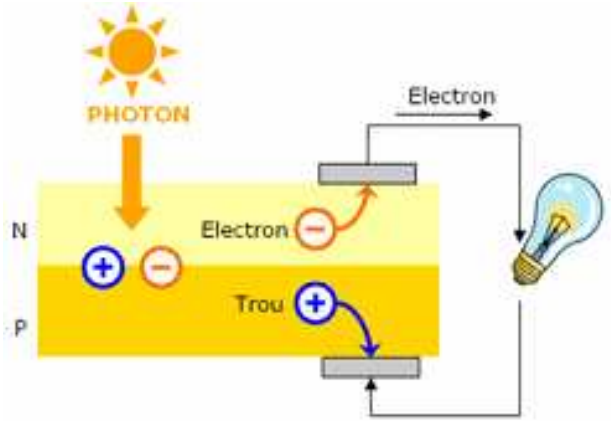
➢ *Laser to improve Side-Channel attacks*

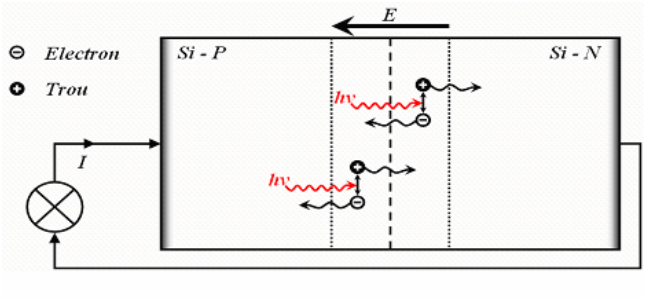
- Background
- Experimental setup
- Results

Laser in Failure Analysis



Laser - Photoelectric effect :

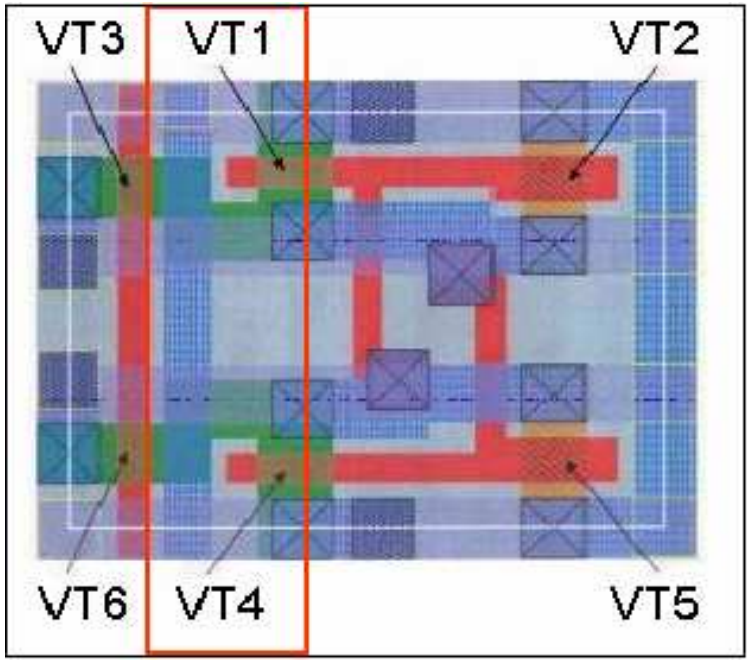




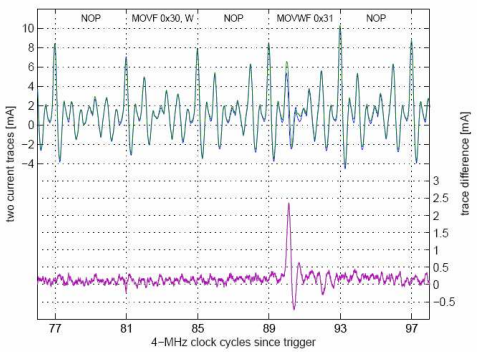
- Many techniques were developed in failure analysis using the 2 laser effects:
  - Thermal effect with a 1340 nm Laser (OBIRCH, TIVA, SEI…)
  - **Photoelectric effect with a 1064 nm Laser (OBIC, LIVA, SCOBIC…)**

S. Skorobogatov *: « Optically Enhanced Position-Locked Power Analysis »*

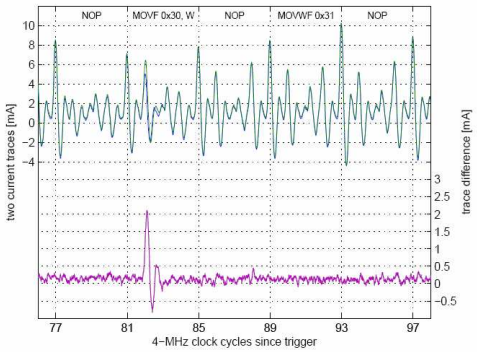
- Spot Laser between 2 transistor of a SRAM cell:
  - **Increasing** power consumption of transistors targeted (local) inducing a global increase of the circuit



Layout of an SRAM cell



Write: (0x00→0xFF) and with laser on VT1+VT4

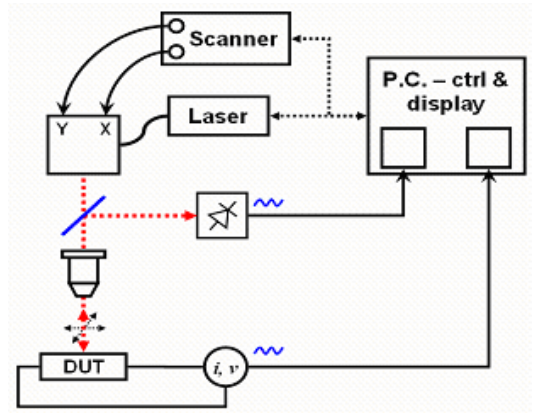


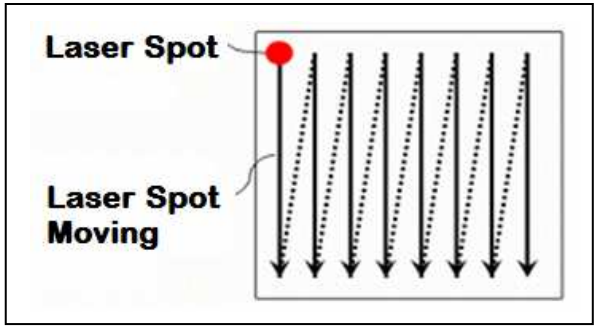
Read: (0xFF) and same with laser on VT1+VT4

Laser source : 639 nm Power : 1 to 3 mW

S. Skorobogatov: Optically Enhanced Position-Locked Power Analysis. Cryptographic Hardware and Embedded Systems Workshop (CHES 2006)

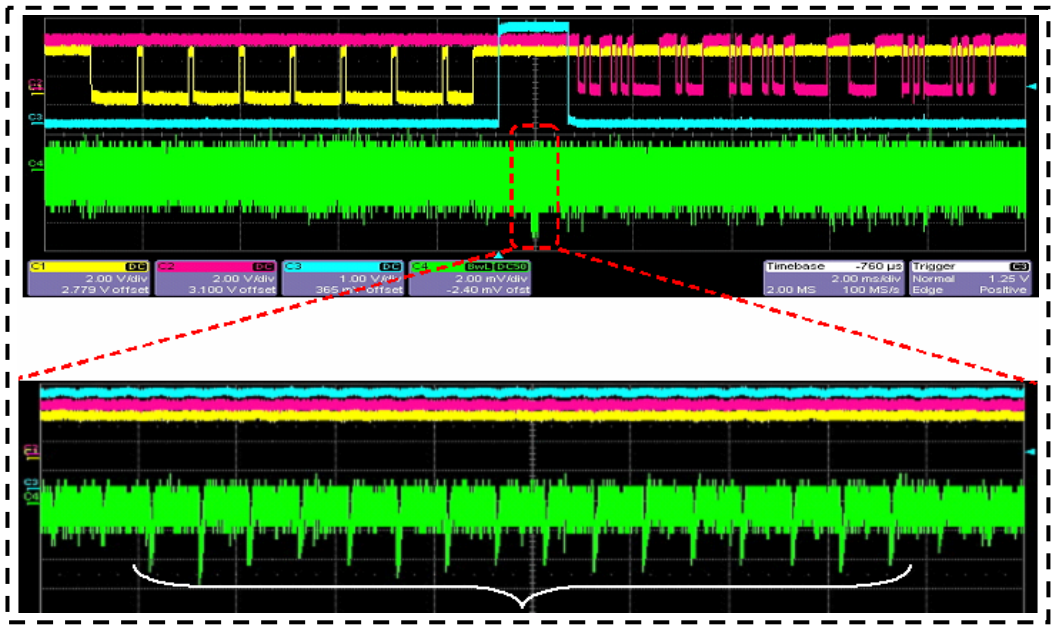
DCG Systems Meridian 1



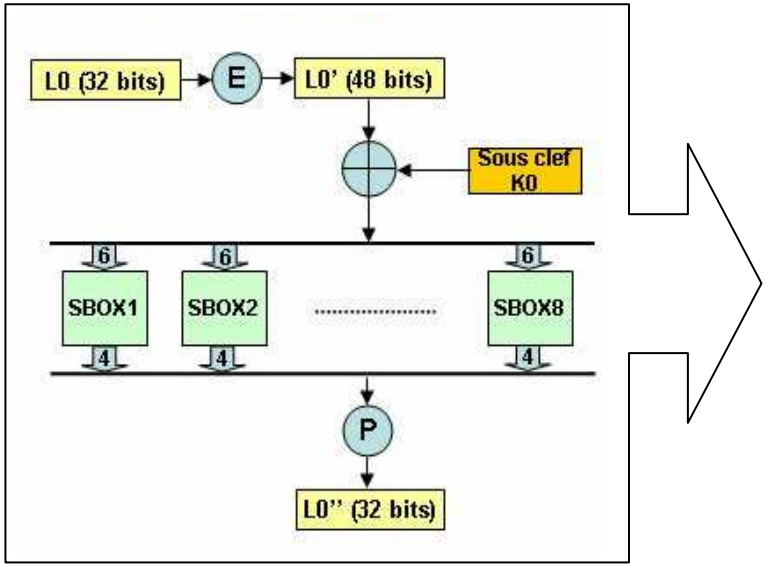


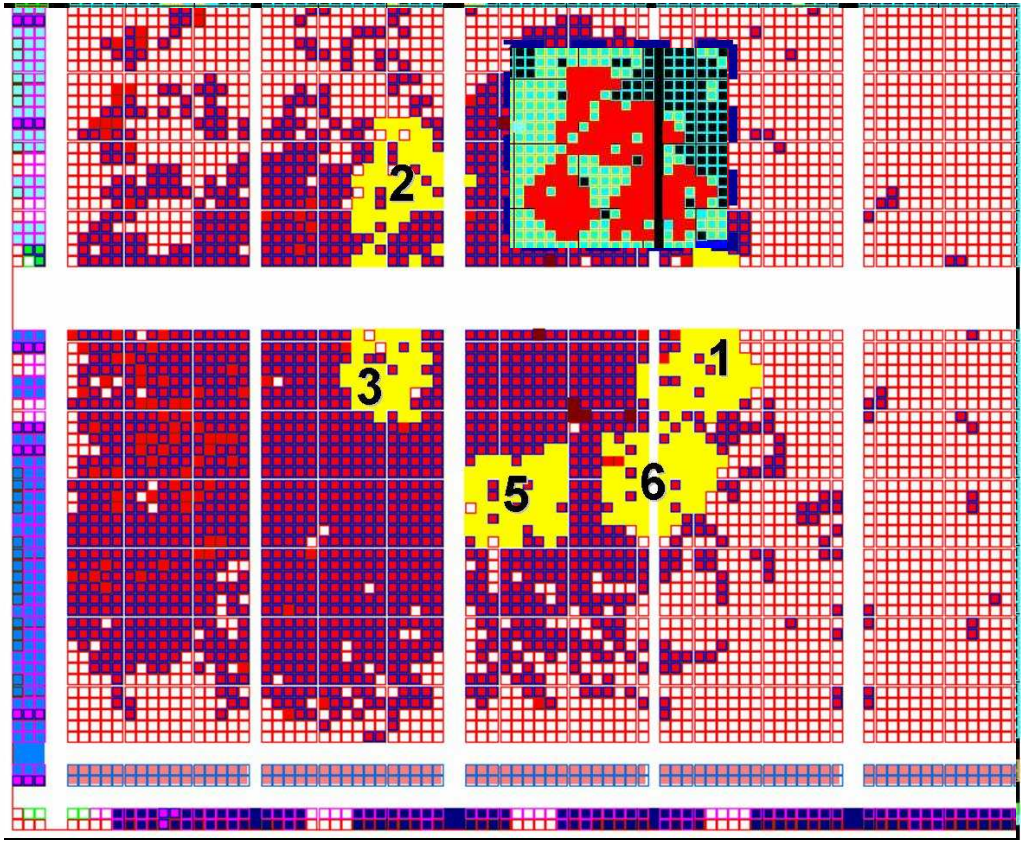
- ***Laser selection :*** *1064 nm (Photo-electric)* ***/*** *1340 nm (thermal)*
- *Analytical capability for 45 nm.Inverted platform for easy ATE direct docking*
- ***Laser Scanning Microscope*** *(LSM) for static and dynamic analysis*

- ***1st step*** : power consumption acquisition **without** laser stimulation on 16000 random messages.
- ***2nd step*** : power consumption acquisition **with** laser stimulation on same messages (same conditions).
- ***3rd step*** : Comparison of the minimum number of curves necessary to perform a successful DPA attack with & without laser stimulation.



Challenges





Laser source : 1064 nm
Power : 10 to 12 mW

- Scanning laser of the area containing **SBOX 4,7 & 8** : local increase of the consumption
- Scanning laser in continuous until obtaining **16000 traces**

DPA Results Laser ON / OFF

- Comparison between both DPA results with and without laser stimulation and numbers of curves necessary to perform the attack

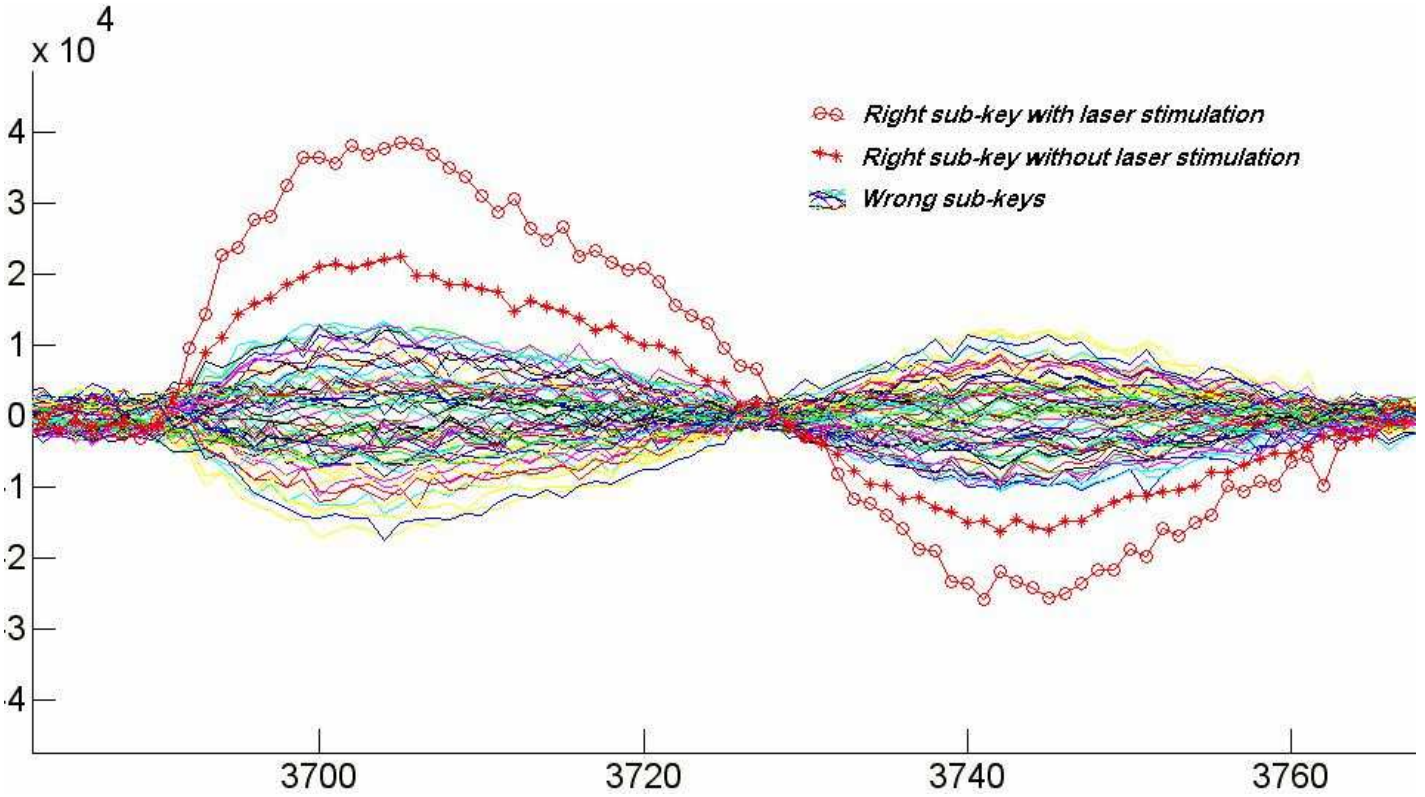
	Bit 0		Bit 1		Bit 2		Bit 3	
Laser state	OFF	ON	OFF	ON	OFF	ON	OFF	ON
SBOX 4	~ 11000	~ 6500	~ 11500	~ 6500	NO	~ 9000	NO	~ 9500
SBOX 5	NO	~ 14500	~ 10000	~ 9500	NO	NO	NO	NO
SBOX 6	~ 11500	~ 9500	~ 10000	~ 7500	NO	NO	NO	~ 12500
SBOX 7	NO	~ 9000	NO	~ 8500	~ 10500	~ 6500	~ 11500	~ 6500
SBOX 8	NO	NO	NO	NO	~ 12000	~ 9500	~ 13500	~ 10000

- Conclusive results on ***SBOX 4, 6, 7*** and inconclusive on ***SBOX 5, 8***

On SBOX 4,7 number of curves required are decreased by approximately 1/2

Amplitude comparison

- **Amplitude** comparison between differential curves on the right key, with and without laser stimulation (DPA in 16000 curves on bit 0 of SBOX 4)



Conclusion

	Benefit	Drawbacks
Light Emission	■ Static acquisition : • Cipher localization • Spy memory activity ■ Dynamic acquisition (TRE) : • Probe internal signal • Recover a subkey from DES	■ Acquisition method : Each messages need to be integrated on time to obtain a significant TRE curves. ■ Lack of resolution on latest techno ■ Sample preparation ■ **Equipment cost** : ≈ 2 M€
Laser stimulation	■ Local increase of the power consumption ■ Reduce the number of power consumption curves necessary to perform an attack	■ Need a partial knowledge of the design / implementation ■ Sample preparation ■ **Equipment cost** : ≈ 500 K€

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

Contact **:**

jerome.dibattista@cnes.fr