THALES

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

cnes

Dynamic light emission technique for optical side channel method

Jérôme Di-Battista, Martin Hlaváč (Charles Univ.), Jean-Christophe Courrege (Thales), Julie Ferrigno (CNES), Bruno Rouzeyre (LIRMM), Lionel Torrès (LIRMM)

Outline

- *Introduction*
  - Thales/CNES presentation
  - purpose
- *Light Emission Technique*
  - Light Emission in IC
  - Photo Emission principle
  - Dynamic light emission
- *Security systems application*
  - Use-It pilot project
  - Example and Possibilities
- *Conclusion*

Common laboratory CNES / Thalès

- **Failure analysis** laboratory
- **Security evaluation** (ITSEF : Information Technology Security Evaluation Facility)

Use-It Activities (PASR 2005 Project)

- **Use-It** : User Supplier European network for Information Technology security
- Targeted to structure the European R&D community in the Information Technology Security domain
- Final Workshop in Toulouse on July, 2007

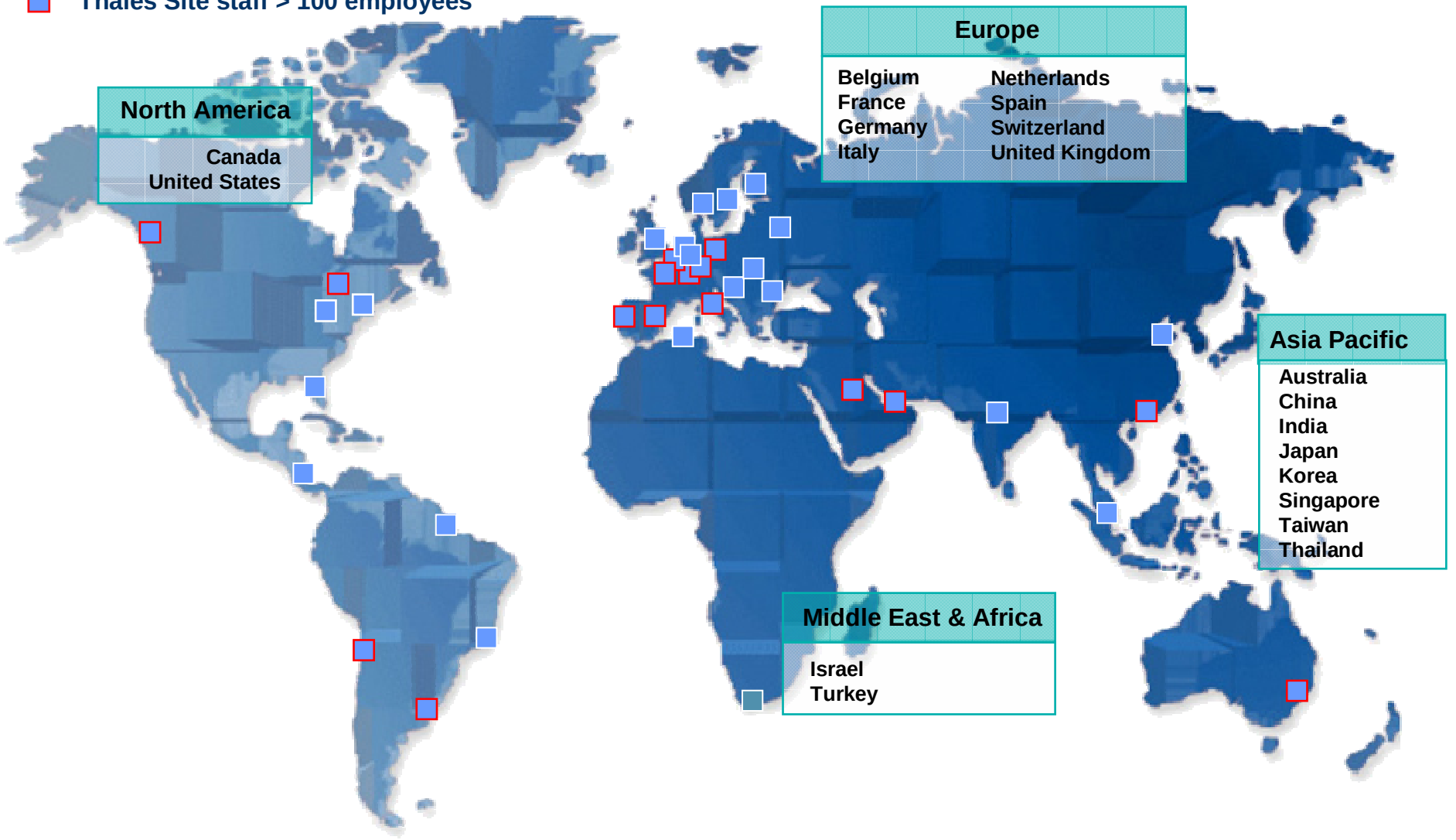
History

1990	**First historical industrial security lab development in 1990 in Rennes**
1994	**Partnership with the CNES** *(French Space Agency)* in Toulouse Evaluation Team expertise starting in 1994, Giving access to one of the best platform in of high end tests in Europe (PICA)
1998	**ITSEF creation** – First accreditation in the French Scheme (DCSSI) CEACI:**C**entre d'**É**valuation & d'**A**nalyse des **C**omposants de l'**I**nformation
1999	**First MasterCard** product evaluation
2000	**First Australian** product evaluated
2001	First Japanese product evaluated SCSUG / VISA PP evaluation (Selected as 1 of 3 ITSEF in the world)
2002	Japanese ITSEF training (Hardware)
2003	Japanese METI organizations training & **Japanese ITSEF training** (Software) First Chinese / Hong-Kong secure product qualification
	First EMV evaluation CAST - **Master Card Agreement** PCI **PED**
2004	E-Government and biometrics, and challenge GIE-CB
2005	Join Thales Security Systems. Definition of an optimized CC evaluation process **First french EAL5+ IC evaluations**
2006	Chronotachygraphe **First french evaluation of an ICAO BAC PP**

An international credible actor

Our Go to market

Thales Site staff > 100 employees



- **Common criteria**
  - Chip manufacturers and Smart Cards OS designers (Atmel, Gemalto)
  - More and more specific application dependent protection profiles
    - Transport, bank, passport (PP BAC & EAC), digital signature (PP SSCD)

- **Private schemes**
  - 70% of evaluation requests
  - MASTERCARD: CAST and PCI PED evaluations
  - GIECB, or Telecom operators

- **Consulting**
  - Pre-evaluation
  - ITSEC or CC dedicated consulting (ST, pre-audit, checklist)
  - Trainings

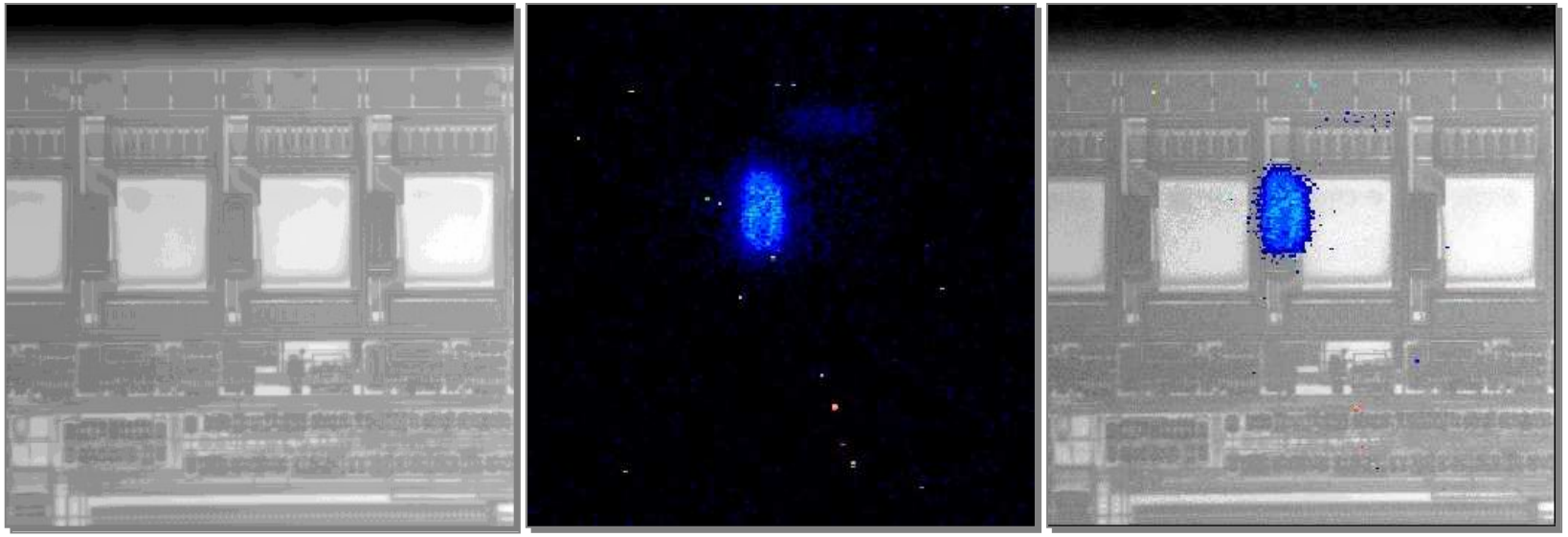
Purpose

- Use of failure analysis tools for security evaluation
- Demonstration of the potential of dynamic light emission for cryptanalysis.
- Shows the perspective following the Use-It pilot project.

Outline

- *Introduction*
  - Thales/CNES presentation
  - purpose
- *Light Emission Technique*
  - Light Emission in IC
  - Photo Emission principle
  - Dynamic light emission
- *Security systems application*
  - Use-It pilot project
  - Example and Possibilities
- *Conclusion*

Light emission (EMMI)

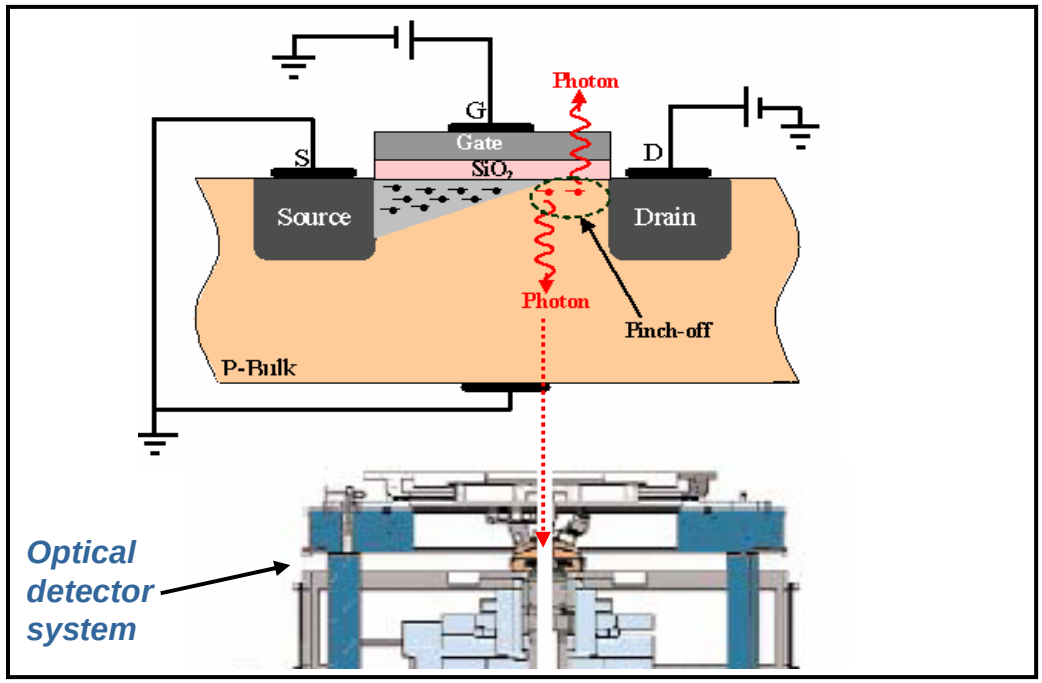


Protection Diode directly biased (enlarging = 20X; silicon thickness = 400 µm)

- **Emission from saturated junction**
- **Fault localization**

Photo Emission Principle

nMOS transistor



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

Photon emission dependencies :

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

detector system

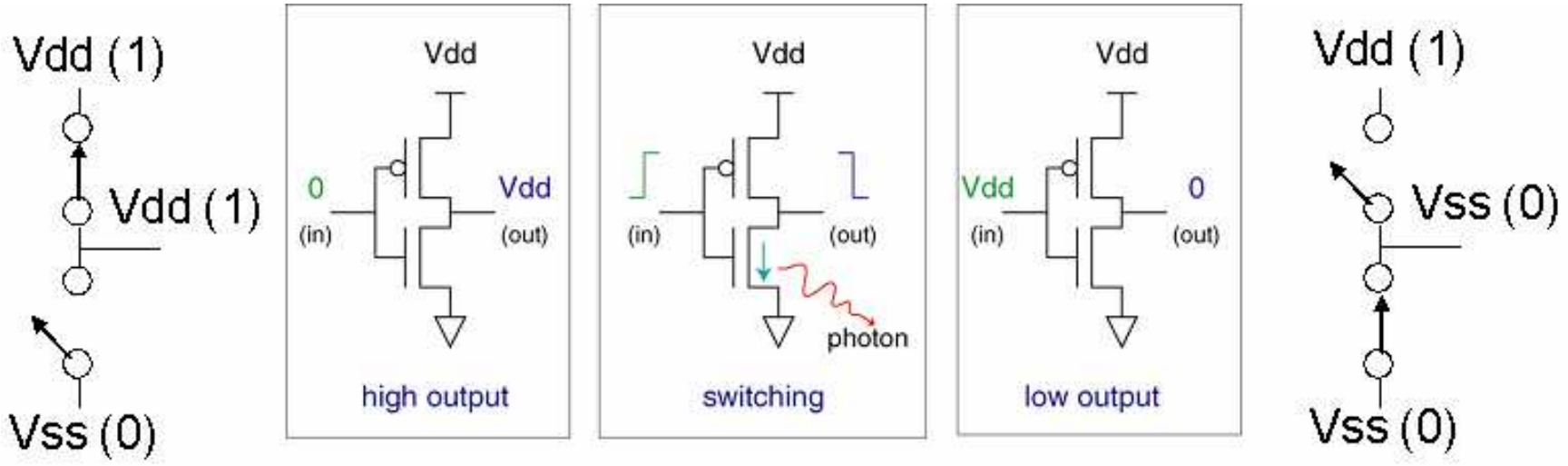
- ✓**CCD silicium captor wavelength: λ = 400 – 1200 nm**

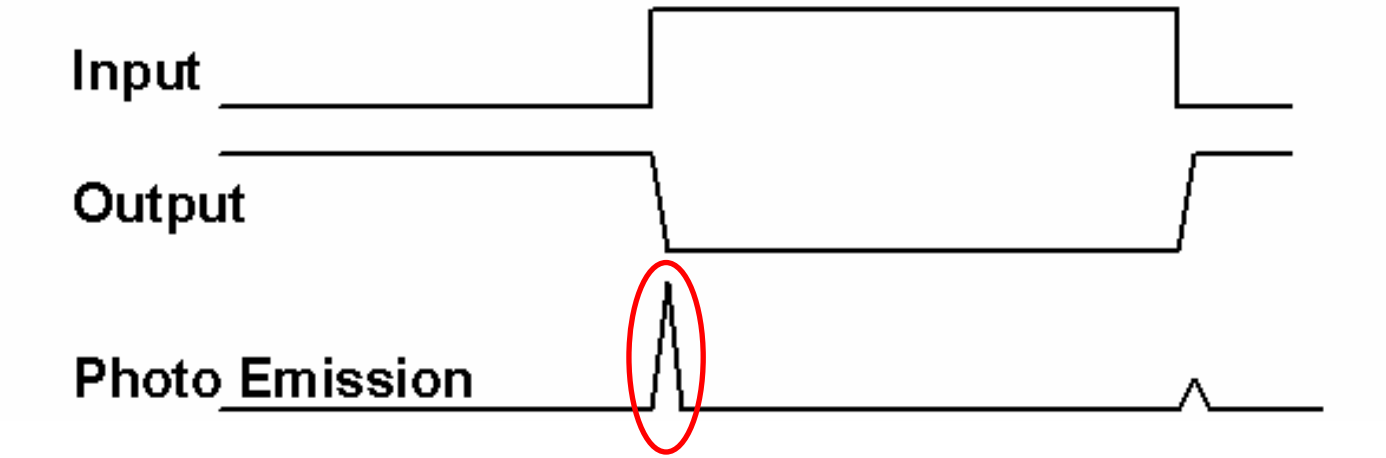
or

- ✓**CCD HgCdTe captor wavelength: λ = 900 – 1500 nm**

(**Infrared : λ = 500 – 1000 nm**
Visible : λ = 400 – 700 nm)

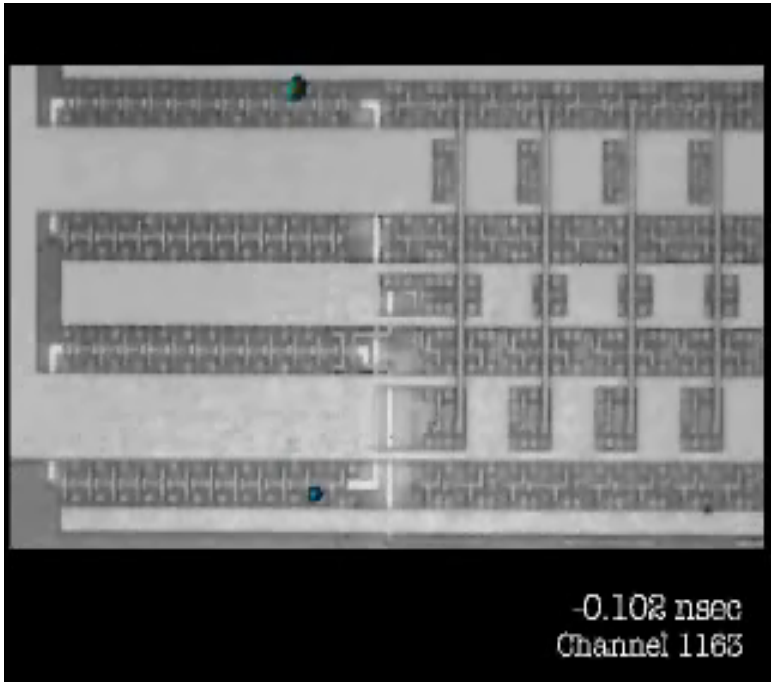
Dynamic Photo Emission Principle



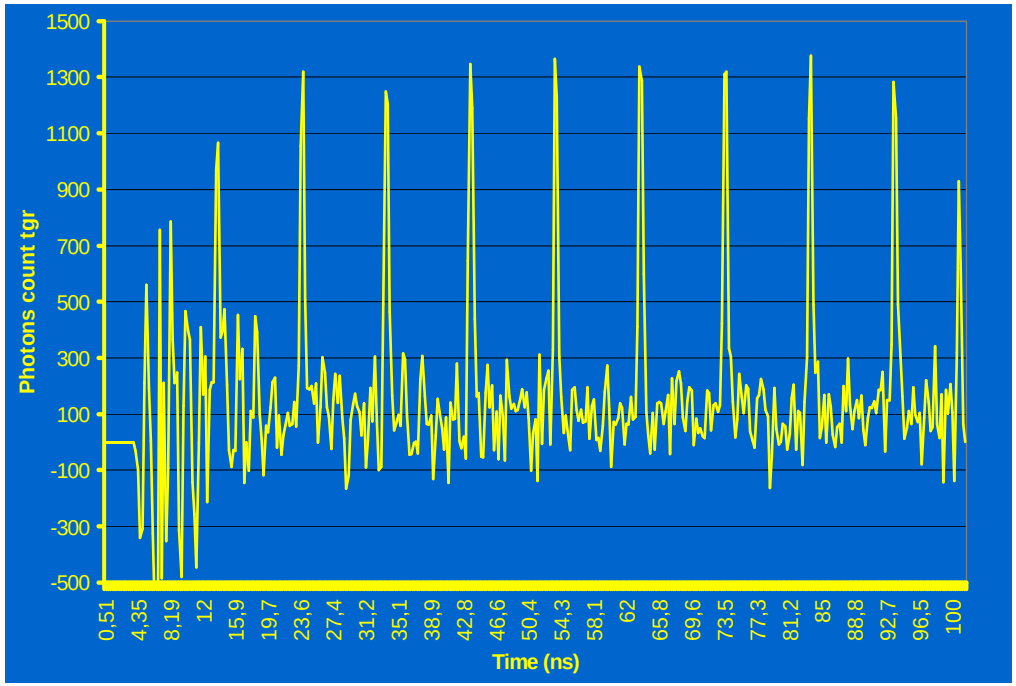


Dynamic Light Emission Technique

Dynamic Light emission (PICA and TRE)



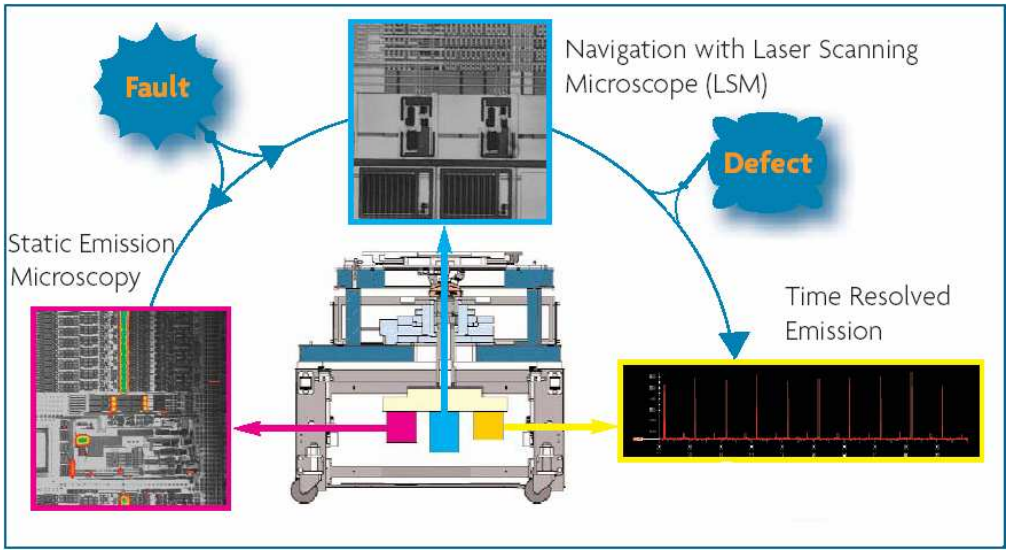
PICA (Picosecond Imaging circuit analysis)



TRE (Time Resolved Emission)

- Saturation occurs briefly during commutation
- Allows to follow the electrical signal propagation
- Direct probing of sensitive data

Testing devices and Tools



OPTICA by Credence

- **Static and Dynamic Emission Microscopy**

- **Mepsicron II detector**
- **Spatio-temporal (e.g. (x,y) @ t)**
- **Visible to 900nm Spectral Range**
- **Probing specific area**

Outline

- *Introduction*
  - Thales/CNES presentation
  - purpose
- *Light Emission Technique*
  - Light Emission in IC
  - Photo Emission principle
  - Dynamic light emission
- *Security systems application*
  - Use-It pilot project
  - Example and Possibilities
- *Conclusion*

Goal :

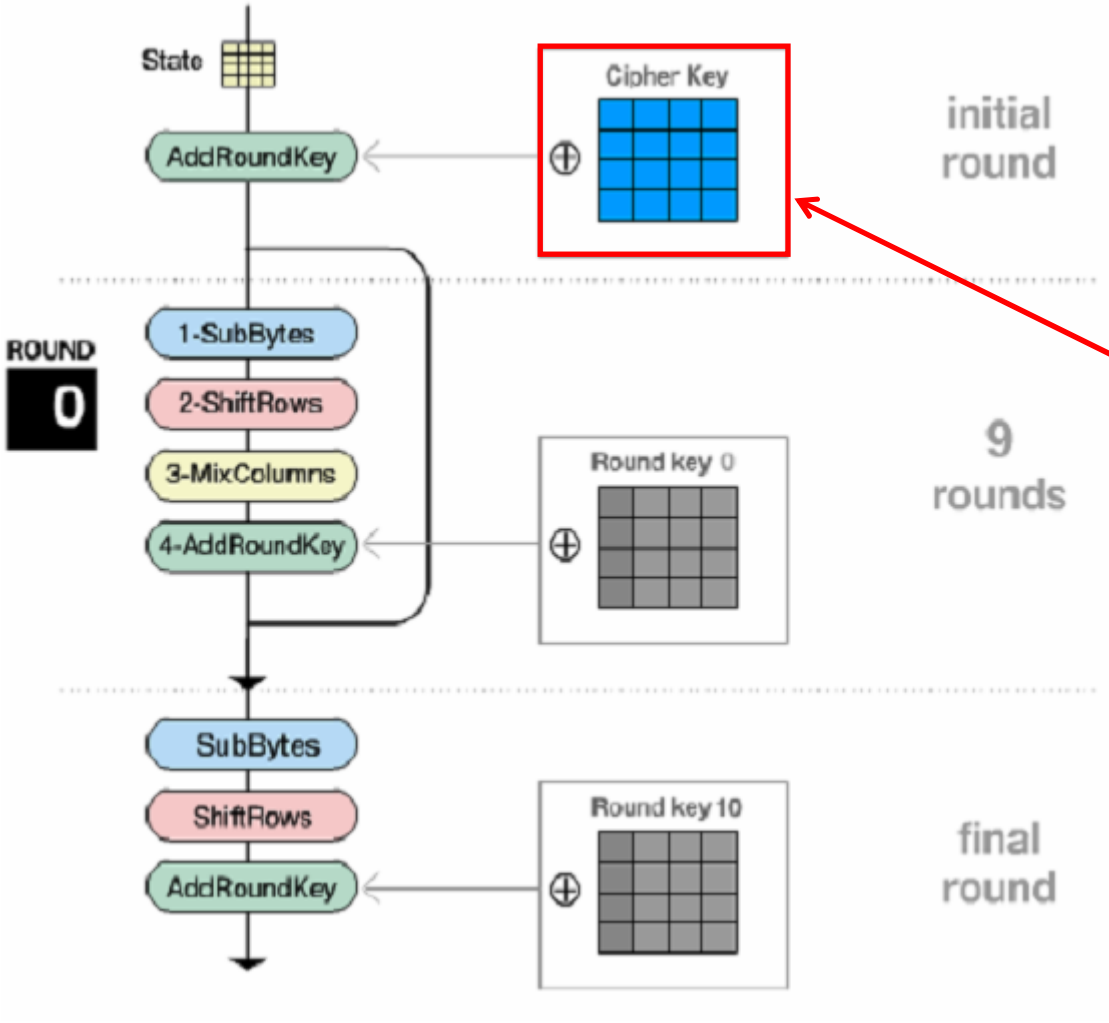
- **Demonstration of the potential of dynamic light emission for cryptanalysis.**

How :

- **Implemention of a « naive » AES on a µcontroller (PIC16F84A - Gold Card) open in backside, to try to recover the secret key through dynamic light emission acquisition**
- **Join work between Charles University (Prague), CNES and Thales Security Systems (Toulouse)**

µcontroller open in backside

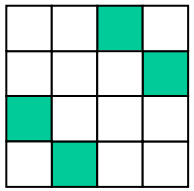
AES : Advanced Encryption Standard



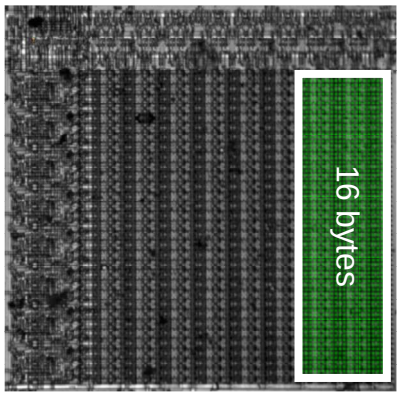
Sensible Round key selected for light emission observation

Measurement goal

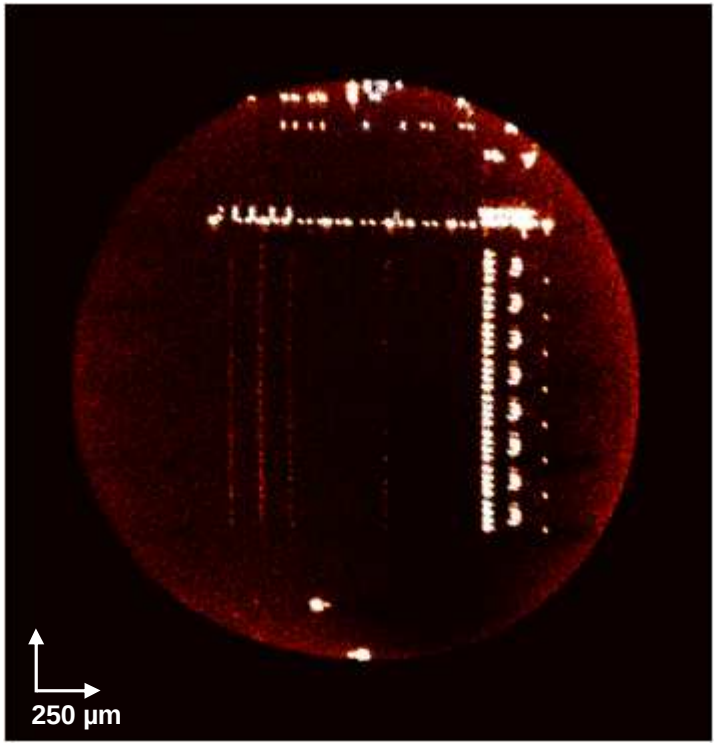
AES state



16 bytes



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



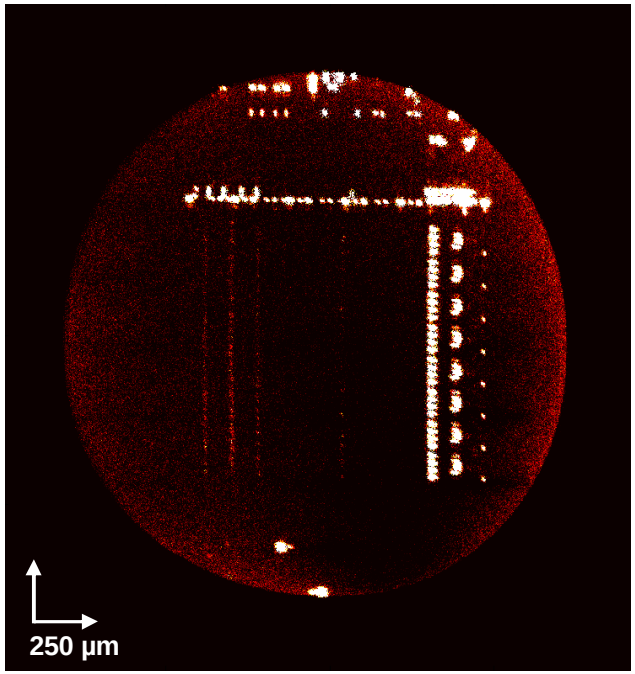
Monitor the changes on the bytes in State block during AES encryptions.

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

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

byte stays => just noise

Static vs. dynamic observation



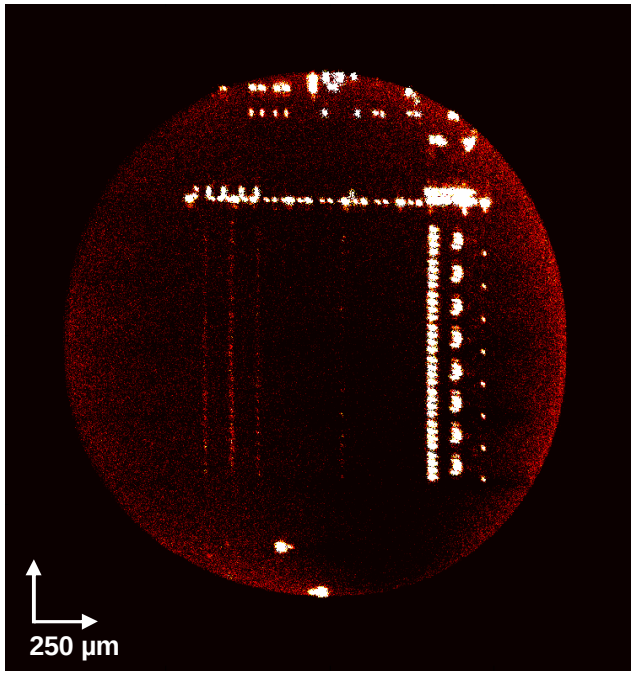
All photons observed in one image

vs.

```
MAIN_LOOP
   movlw   0xff
   xorwf   block+0x0,f
   movlw   0xaa
   xorwf   block+0x0,f
   movlw   0x55
   xorwf   block+0x0,f
   movlw   0x00
   xorwf   block+0x0,f
   call    SEND_TRIGGER
   goto    MAIN_LOOP
```

Frames
166 ns = 1 clock cycle

Static vs. dynamic observation



All photons observed in one image

vs.

Frames
166 ns = 1 clock cycle

Dynamic Observation results

At byte level :

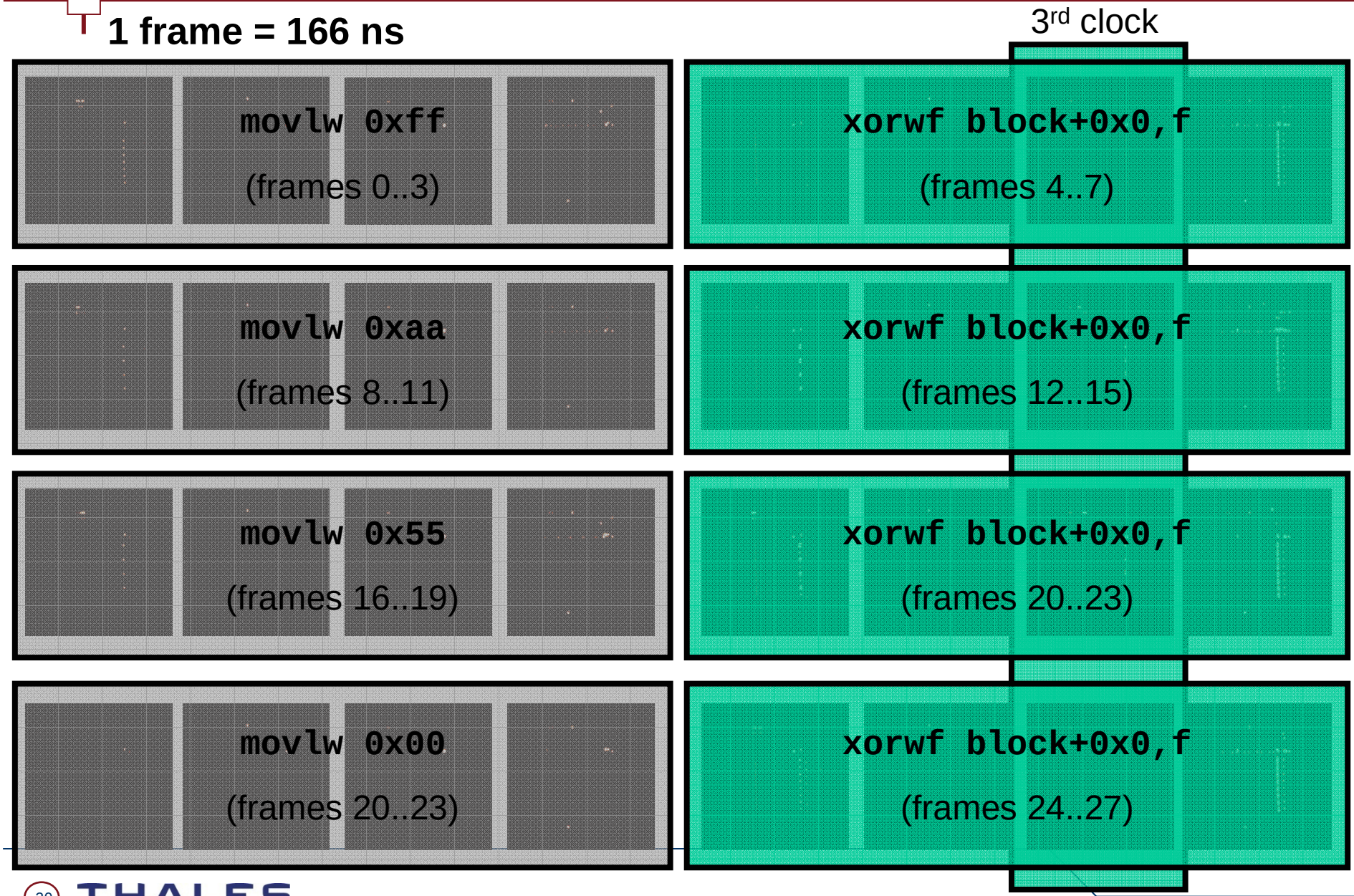
- **Search for collisions so that byte X of the AES does not change during MixColumns operation of the first Round**
- **Occurrence probability 1/16**
- **With 256 such messages + some cryptanalysis we recover the complete key**

At bit level :

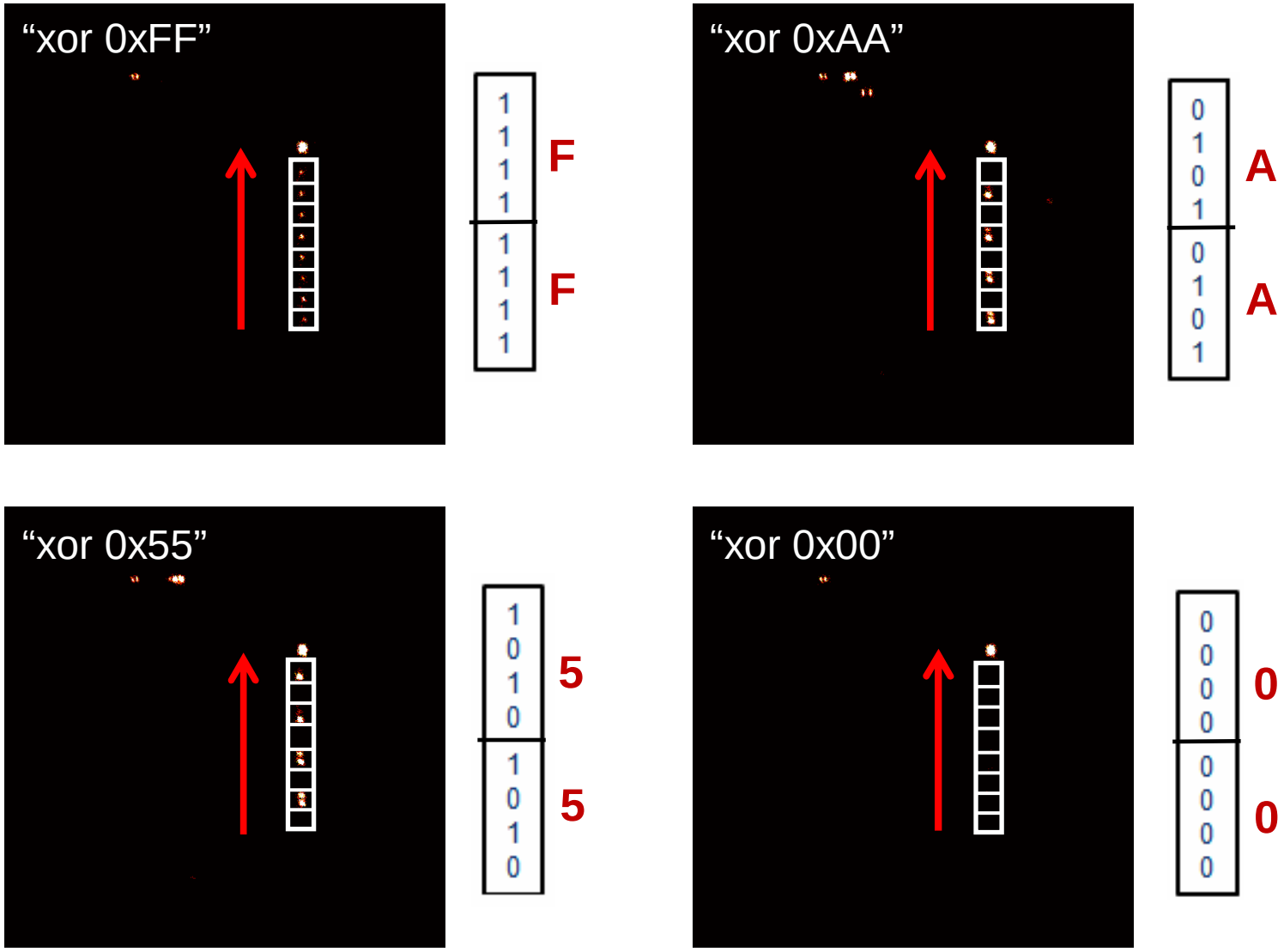
- **Analysis the output of the first XOR between the message and the Key =** addrounkey **operation in 1st round**
- **Recovering of the key with one execution**

Individual frames

1 frame = 166 ns



3rd clocks reveal the key



Outline

- *Introduction*
  - Thales/CNES presentation
  - purpose
- *Light Emission Technique*
  - Light Emission in IC
  - Photo Emission principle
  - Dynamic light emission
- *Security systems application*
  - Use-It pilot project
  - Example and Possibilities
- *Conclusion*

Dynamic light emission :

- **Very strong side channel observation**
- **Applicable on other ciphers/schemes and devices**
- **Can be done without layout knowledge (partial reverse engineering can be done through EMMI)**

Drawbacks :

- **Very expensive**
- **Limited because of synchronization problems**
- **Needs physical access to the chip by non trivial IC preparation (back side thinning)**

… Anyway we have proven the potential of dynamic light emission technique for security purpose

Acknowledgments

- Thank you for your attention
- Questions?

Contact :

Jerome.dibattista@thales-is.cnes.fr