November 20th, 2025

European Cyber Week

THE SOVEREIGN CYBER & DEFENCE AI FORUM

Optical Techniques

BITFLIP Conference

Optical Techniques

November 20th, 2025
16:00

Le Refectoire

Jean-Max DUTERTRE

Professor, Mines Saint-Etienne

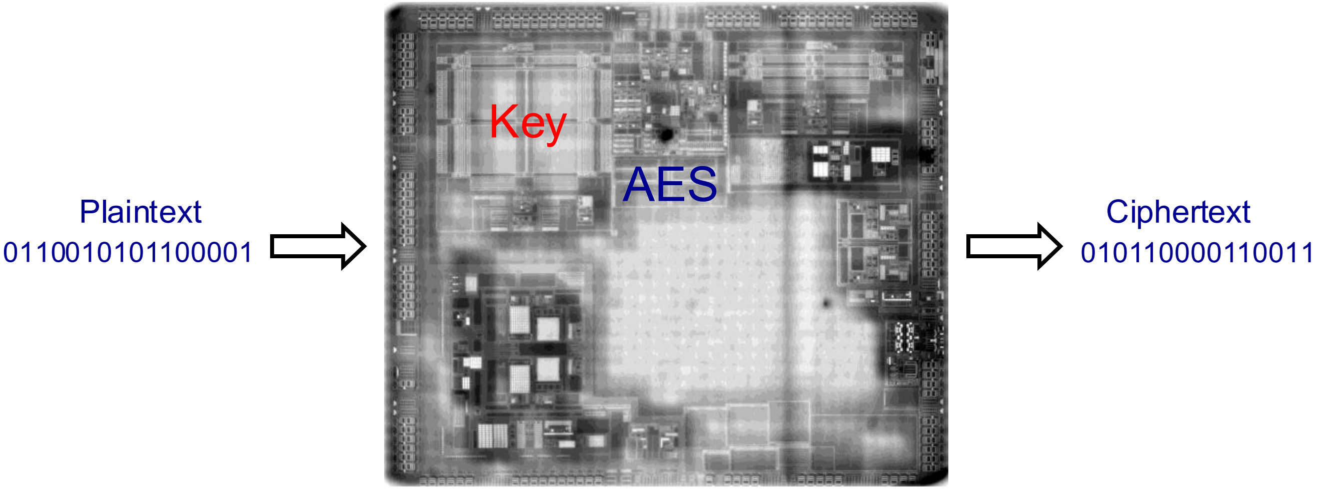
Betrayed by light – Using Photon Emission Microscopy as an Enabler of Laser Fault Injection

H.Perrin, J.-M. Dutertre, J.B. Rigaud

Equipe Commune Systèmes et Architectures Sécurisées
Mines Saint-Etienne, CEA, Leti, Centre CMP
13541 Gardanne FRANCE

Context – Hardware security

- Hardware security – hardware attacks
- Secure HW: integrated circuits implementing security features
  - ✓ MCU with hardware cryptographic accelerator
  - ✓ Memory readback protection (IP & user data protection)



Plaintext
0110010101100001

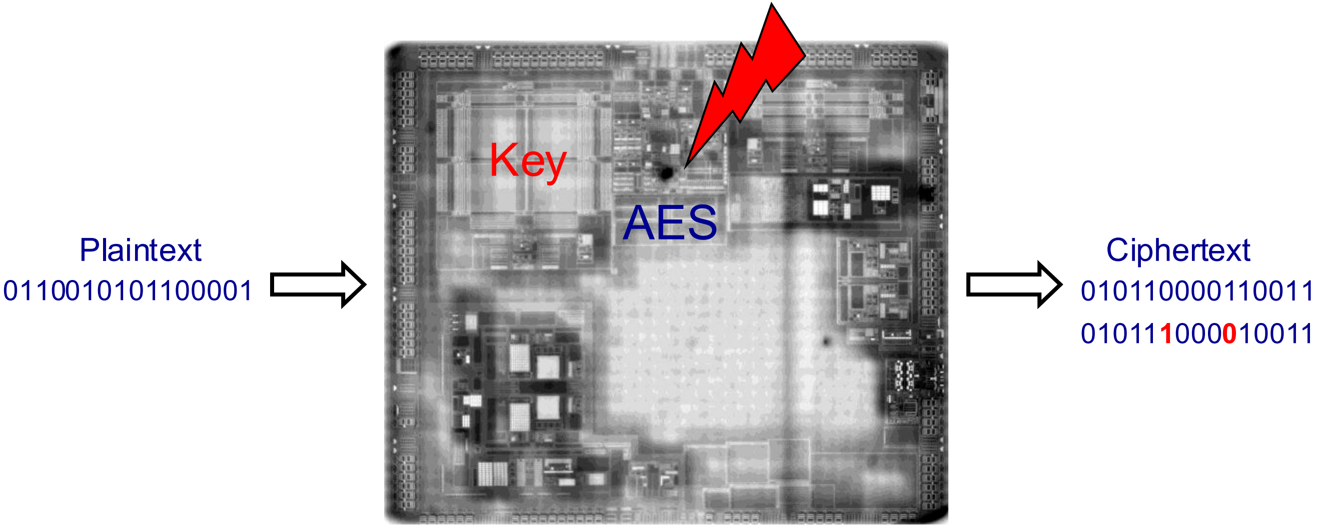
Key

AES

Ciphertext
010110000110011

Context – Hardware security

- Hardware attacks
- Fault injections attacks
  - ✓ Information leakage (DFA) → secret key extraction
  - ✓ Control flow attacks (e.g., test inversion → memory extraction)

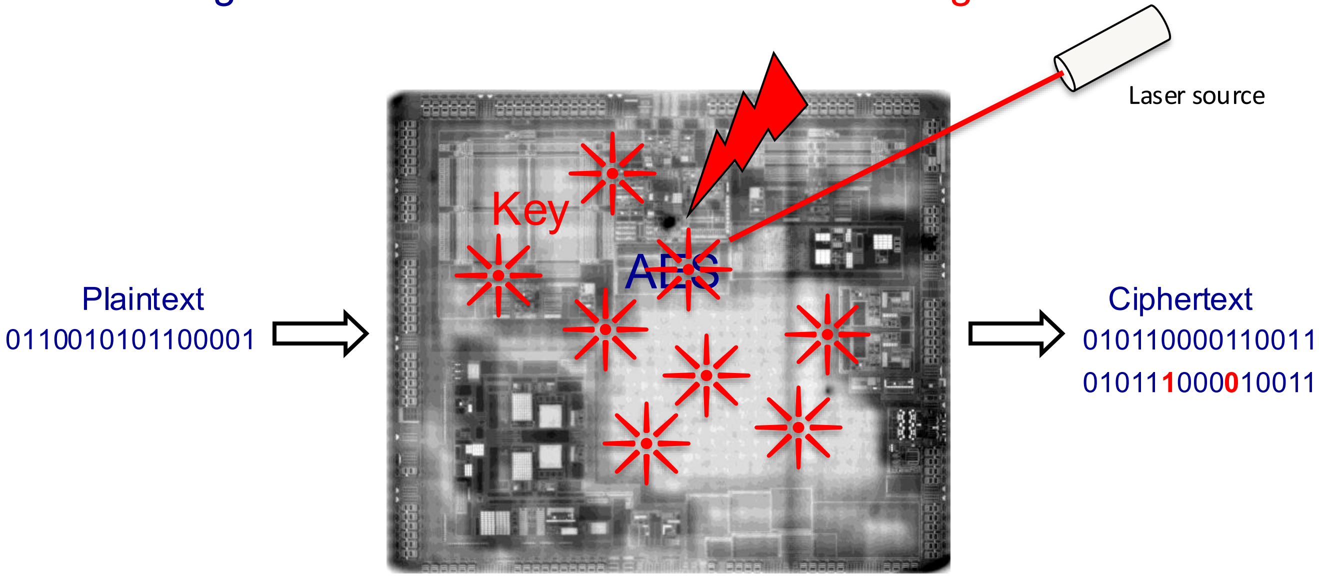


Plaintext
0110010101100001

Ciphertext
010110000110011
010111000010011

Context – Hardware security

- Hardware attacks
- Laser Fault Injection (LFI)
  - ✓ Accurate (µm accuracy) & efficient (bit-set/reset/flip)
  - → Finding the Point Of Interest = time consuming

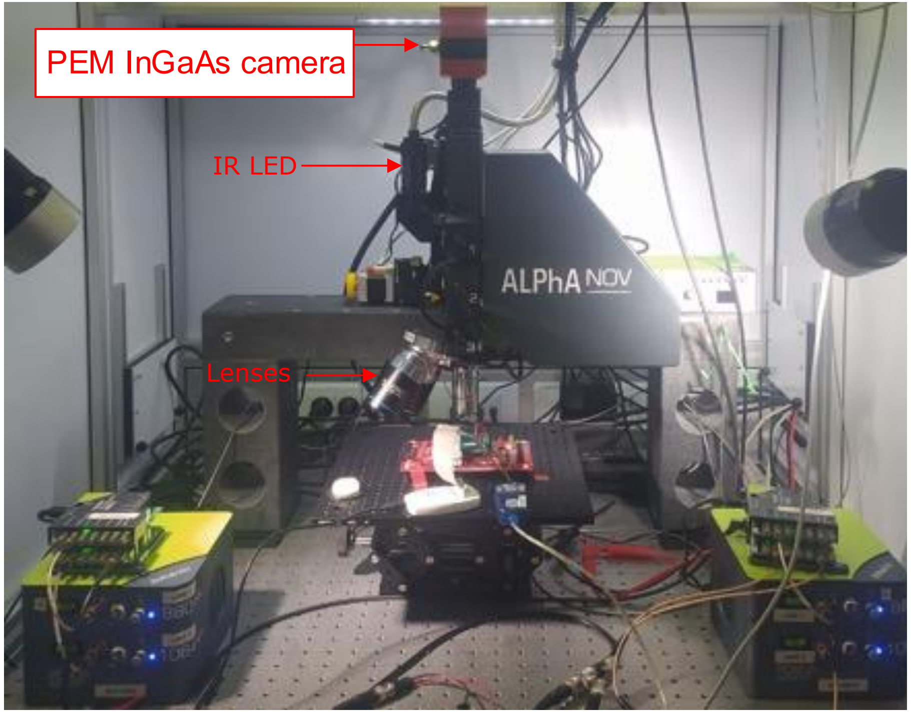


Plaintext
0110010101100001

Ciphertext
010110000110011
010111000010011

This talk

- Failure analysis as a hardware attack facilitation tools?



- FA tool: photon emission analysis
  - ✓ Reverse engineering to accelerate fault injection attacks
  - ✓ LFI: where? and when?
  - → Photon Emission Microscopy PEM

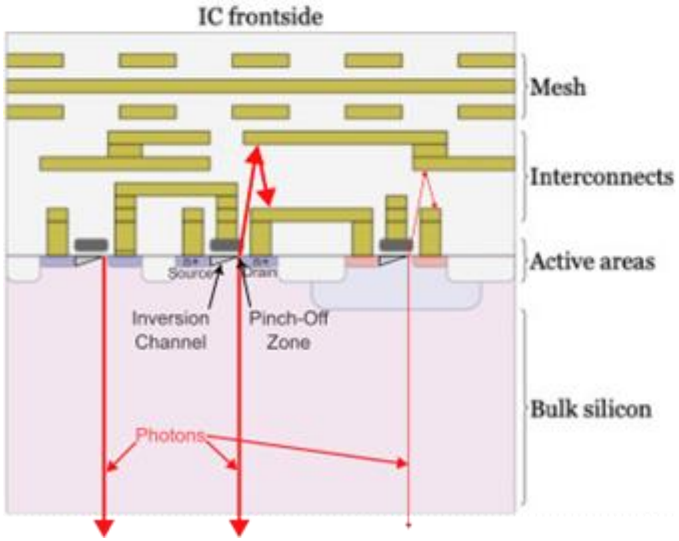
- Q? Use of PEM to accelerate LFI?

Betrayed by light – Using PEM as an Enabler of LFI

- Photon Emission (PE) basics
- PEM setup and imaging methodology
- PEM for LFI facilitation
- Conclusion

PE mechanism

- Photon emission from transistors activity
  - ✓ Source-drain electric field: charge carrier acceleration
  - ✓ Kinetic energy released as photons
  - ✓ MOS transistors in saturation mode (pinch-off channel, drain)
  - ✓ $\text{NMOS}_{\text{emission}} > \text{PMOS}_{\text{emission}}$



[Security of the IC Backside, D. Nedospasov, 2015]

FA tool: default localization (90s)

Also efficient to observe transistors in nominal mode

- ✓ Switching transistors (digital logic)
- ✓ Bias current of analog parts

+ tunneling effects (Fowler-Nordheim)

PE mechanism

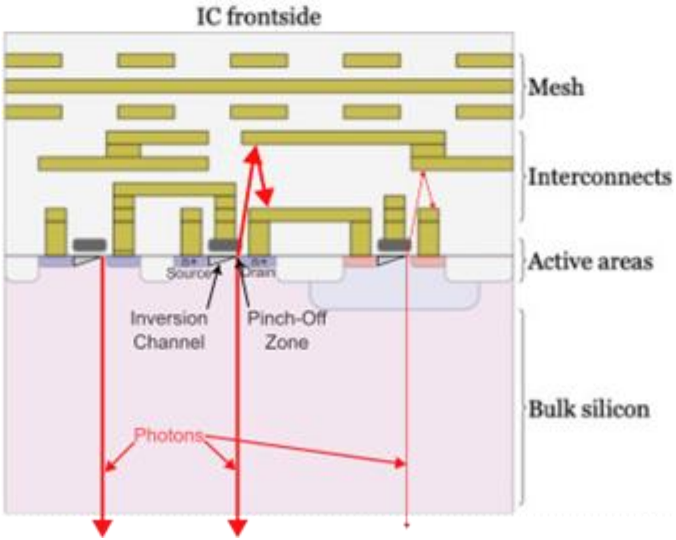
Backside PEM (λ= 1-2 µm)

(to avoid reflection on metal lines and dummies)

- ✓ Si substrate transparent to NIR
- ✓ Substrate thinning improves SNR

Factors favorizing PE

- ✓ Current density
- ✓ V_{DS} voltage

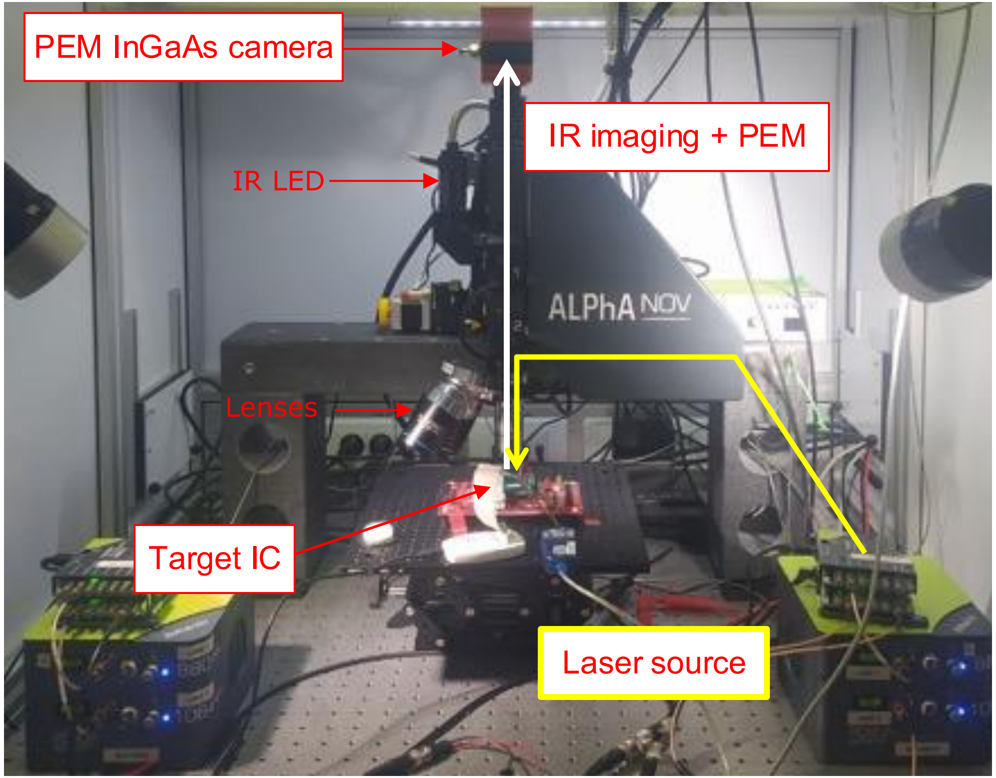


[Security of the IC Backside, D. Nedospasov, 2015]

Betrayed by light – Using PEM as an Enabler of LFI

- Photon Emission (PE) basics
- PEM setup and imaging methodology
- PEM for LFI facilitation
- Conclusion

Photon Emission Microscopy (PEM) setup



Setup:

- ✓ InGaAs camera for PEM + IR imaging
- ✓ LFI

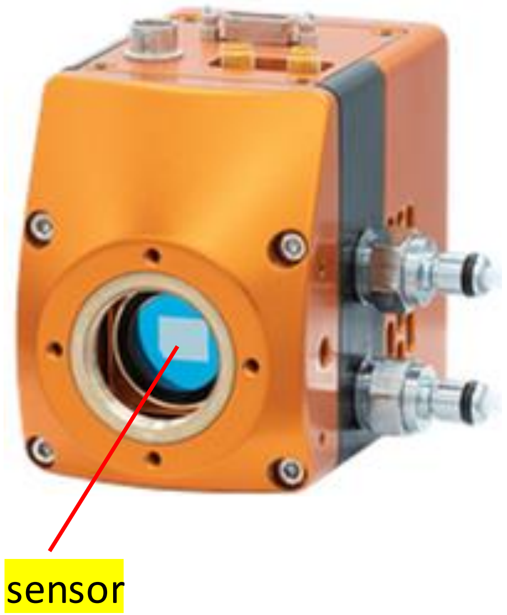
Photon Emission Microscopy (PEM) setup

Photon Emission maps → transistors activity maps

Camera:

✓ 640x512 InGaAs sensor

✓ On a LFI bench



✓ Typical dark current (@-15 °C) : < 750 e^-/p/s

✓ Typical readout noise (rms) : 18 e^-

✓ High sensitivity from λ = 0.6 to 1.7 µm

✓ 15x15µm pixel pitch

✓ Peak Quantum Efficiency : >90% @ 1.3µm

✓ Air-cooled to -15 °C

PEM constraints

Signal to Noise Ratio

✓ Information shall emerge from noise

- PEM: long integration time w.r.t. target's activity

On a running device

→ execution of code loops

⇨

Strong constraints for attack purposes

→ gray box model:

✓ Ability to execute arbitrary code loops

✓ Synchronization

→ Reverse engineering tool

Imaging methodology

Target 1

Microcontroller:

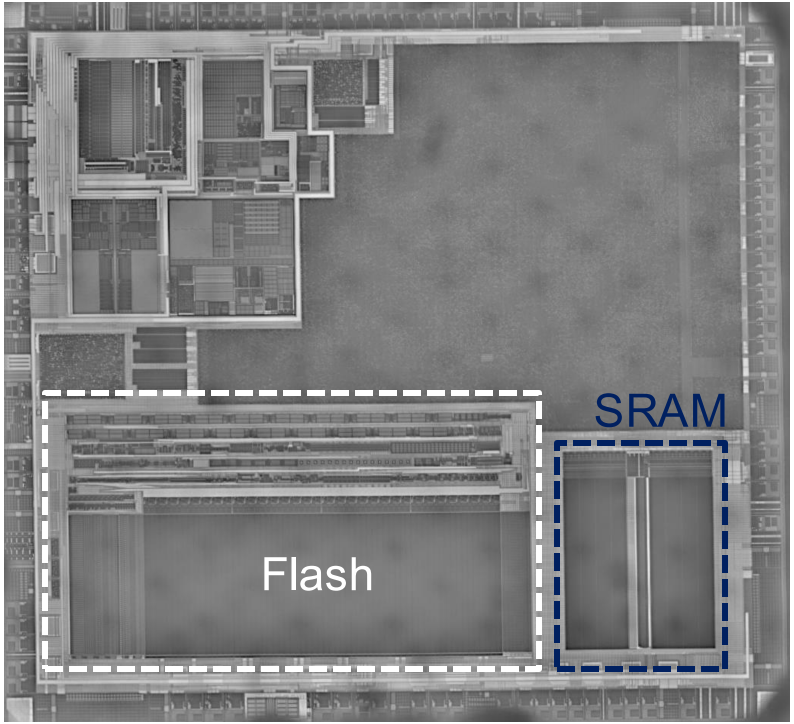
- ✓ ARM Cortex M3
- ✓ CMOS 90 nm
- ✓ 32-bit CPU, 24 MHz
- ✓ 128 kBytes Flash
  page size = 1 kB
- ✓ 8 kBytes SRAM
- ✓ Si thickness: ~350 µm

Si die: 3,000 x 2,500 µm

Flash: 1,400 x 550 µm – 1.3 bits/µm²

SRAM: 245 x 660 µm (x2) – 0,1 bits/µm²

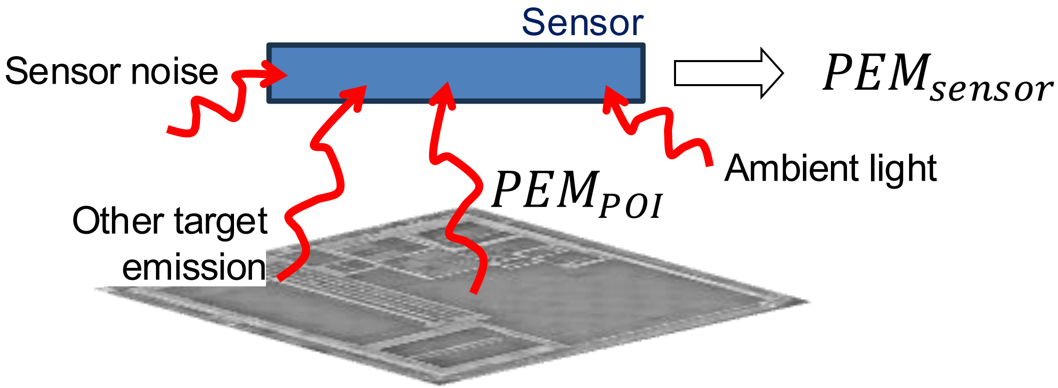
Backside IR view

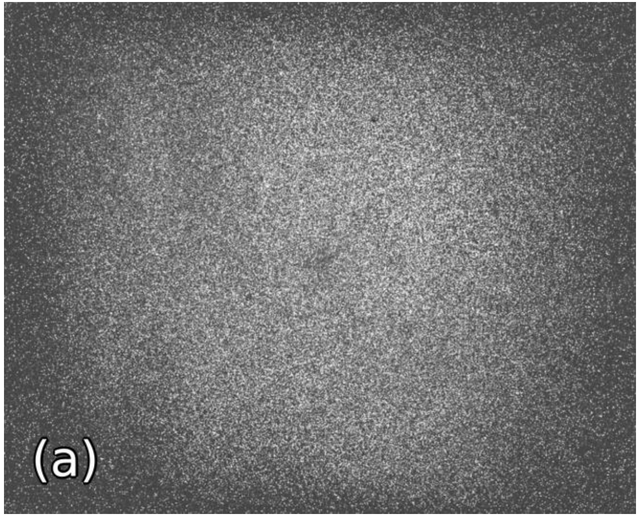


POI = Point Of Interest

Imaging methodology

Signal and noise contributions





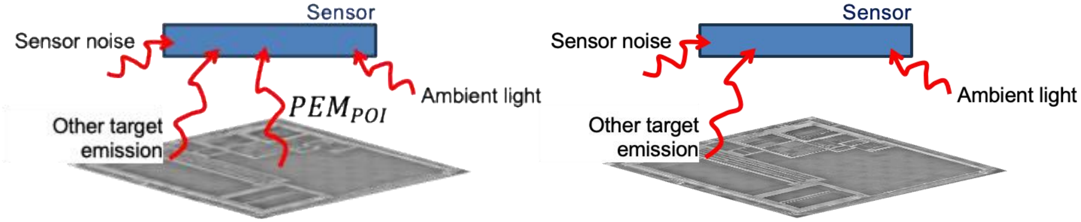
5s exposure, 5x lens, POI active, avg. 20x

Sensor output: $PEM_{sensor} = PEM_{POI} + Noise_{\text{target+sensor+ambient}}$

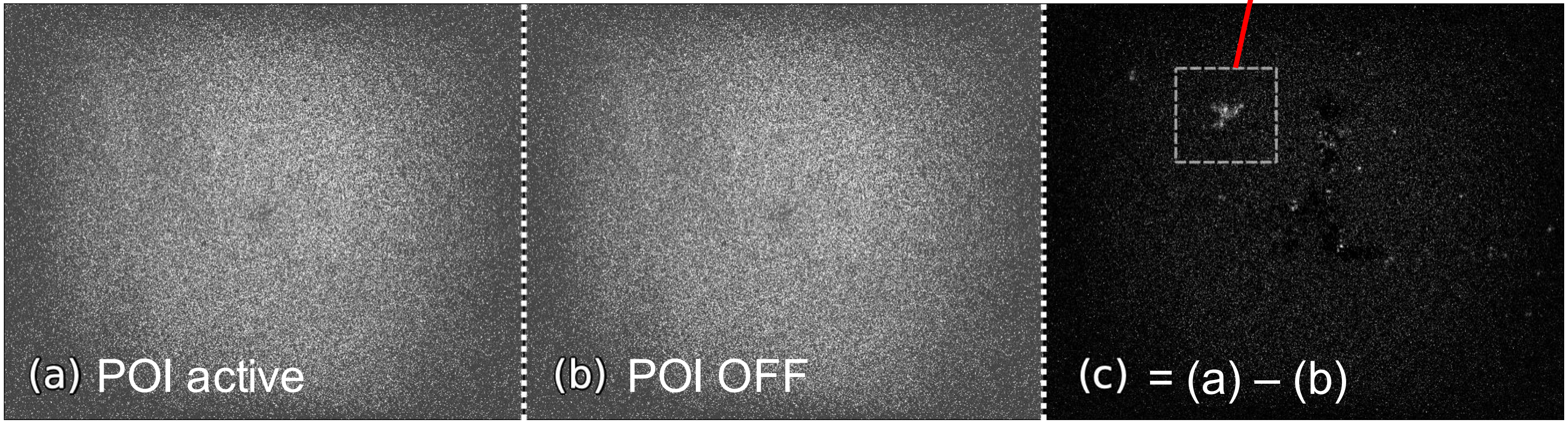
POI = Point Of Interest

Imaging methodology

Differential imaging: PEM$_{\text{POI active}}$ – PEM $_{\text{POI OFF}}$ → POI activity



POI activity



5s exposure, 5x lens, POI active, avg. 20x

Betrayed by light – Using PEM as an Enabler of LFI

- Photon Emission (PE) basics
- PEM setup and imaging methodology

- PEM for LFI facilitation

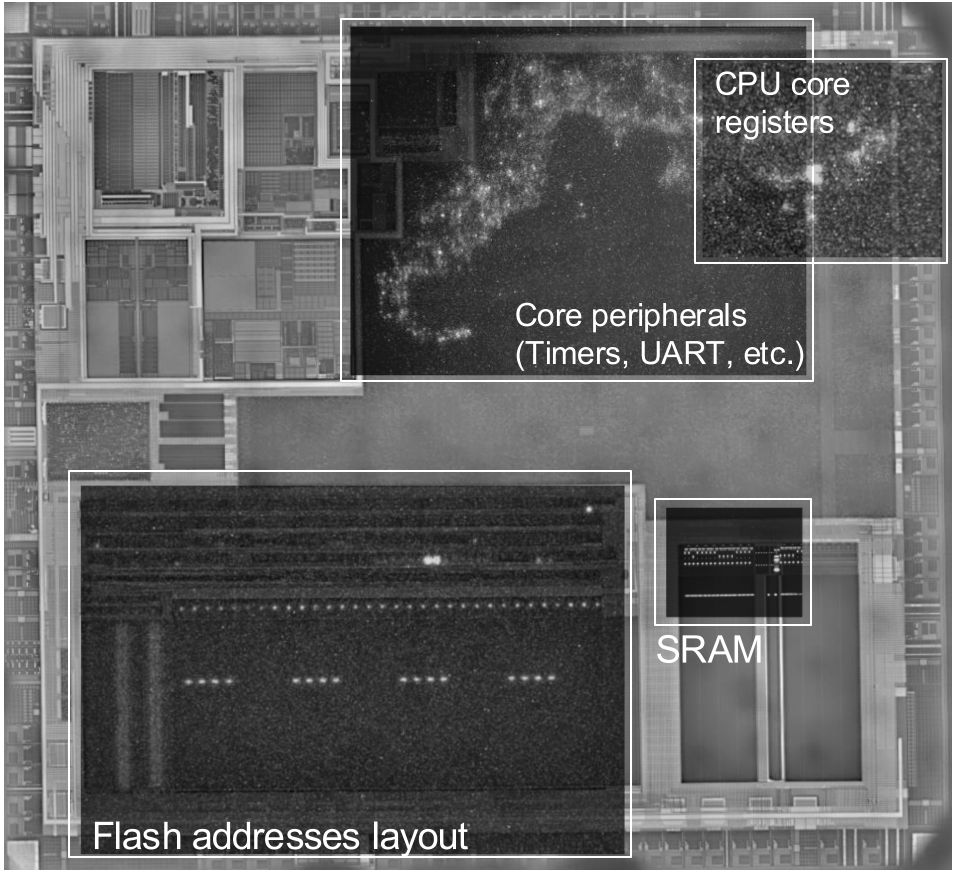
- Conclusion

PEM for LFI facilitation – Reverse engineering

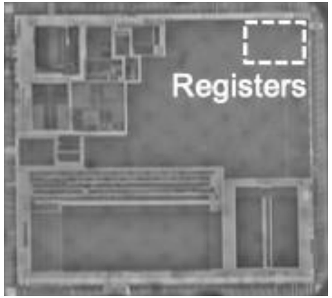
PEM on target 1

- ✓ Quick mapping of target's key elements

Overlay PEM + IR view

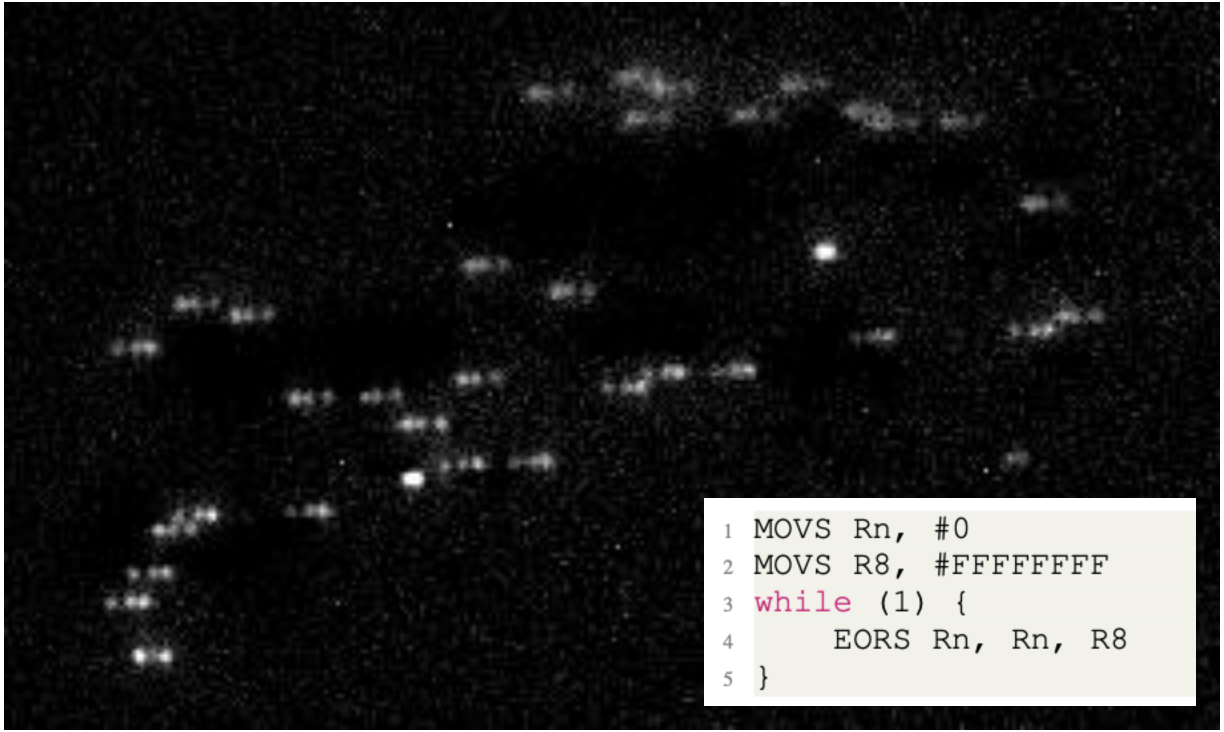


PEM for LFI facilitation – Reverse engineering



PEM on target 1

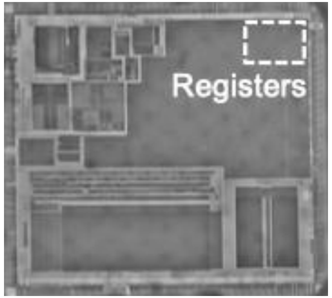
✓ CPU core registers mapping



```
MOVS  Rn,  #0
MOVS  R8,  #FFFFFFFF
while  (1)  {
     EORS  Rn,  Rn,  R8
}
```

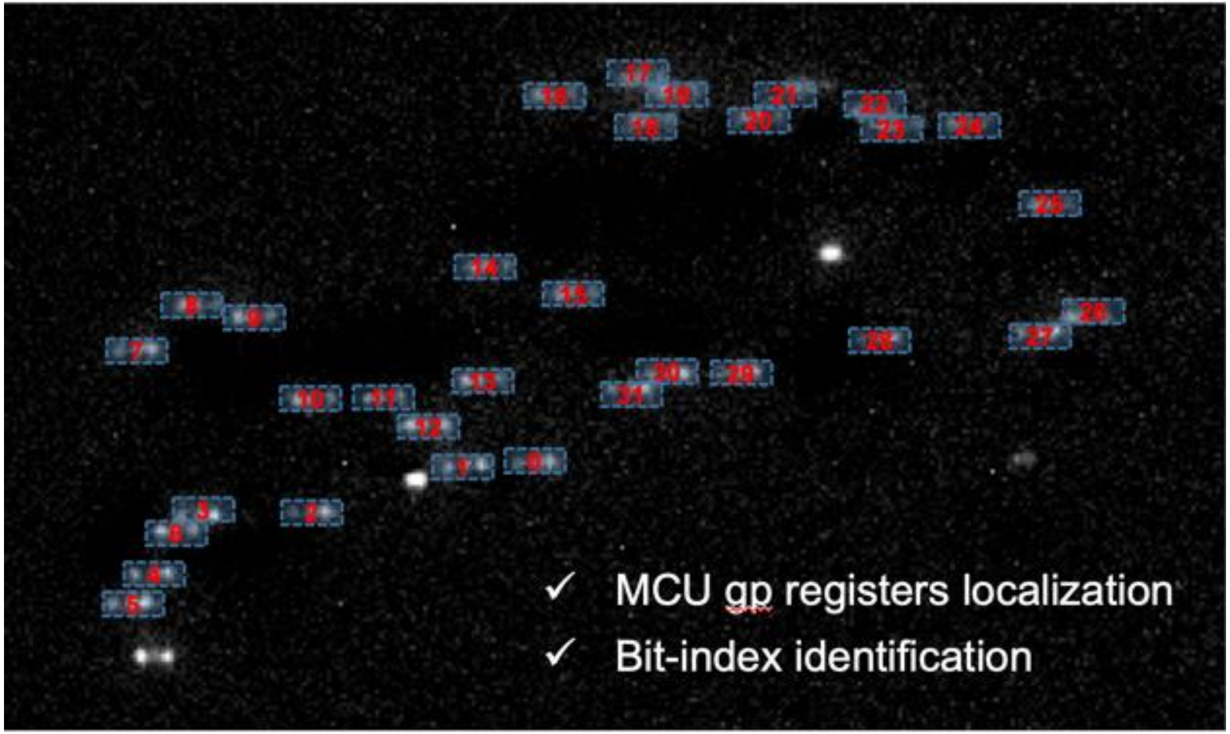
Lens x20, 5s (avg. 5x)
600 Mio. EORS
register R3

PEM for LFI facilitation – Reverse engineering



PEM on target 1

✓ CPU core registers mapping



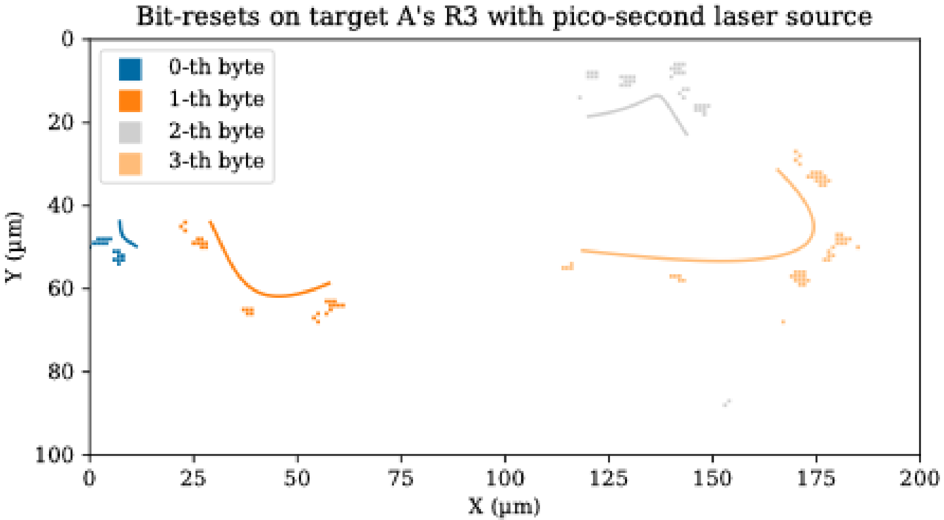
✓ MCU gp registers localization

✓ Bit-index identification

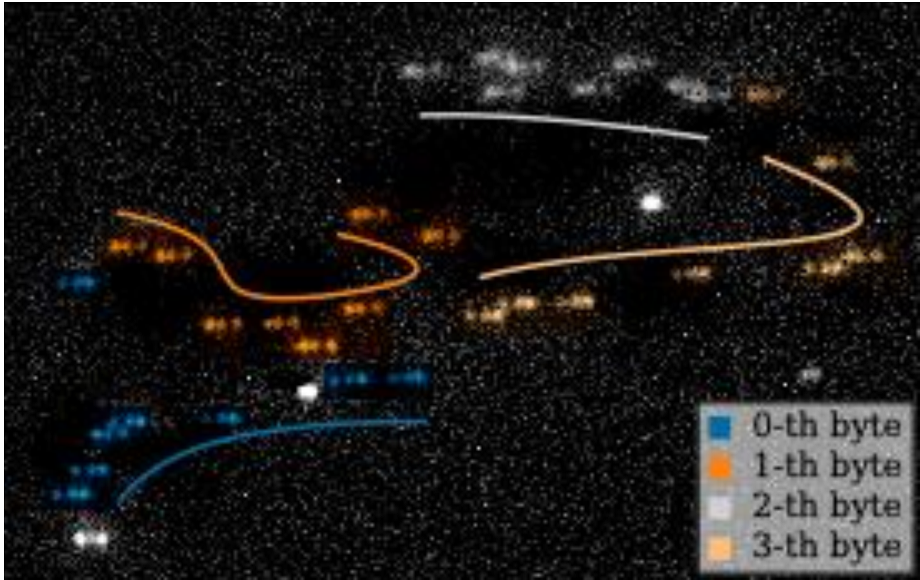
Lens x20, 5s (avg. 5)
600 Mio. EORS
register R3

PEM for LFI facilitation – LFI

LFI from PEM-based register DFFs localization (target 1)



R3 bytes identification

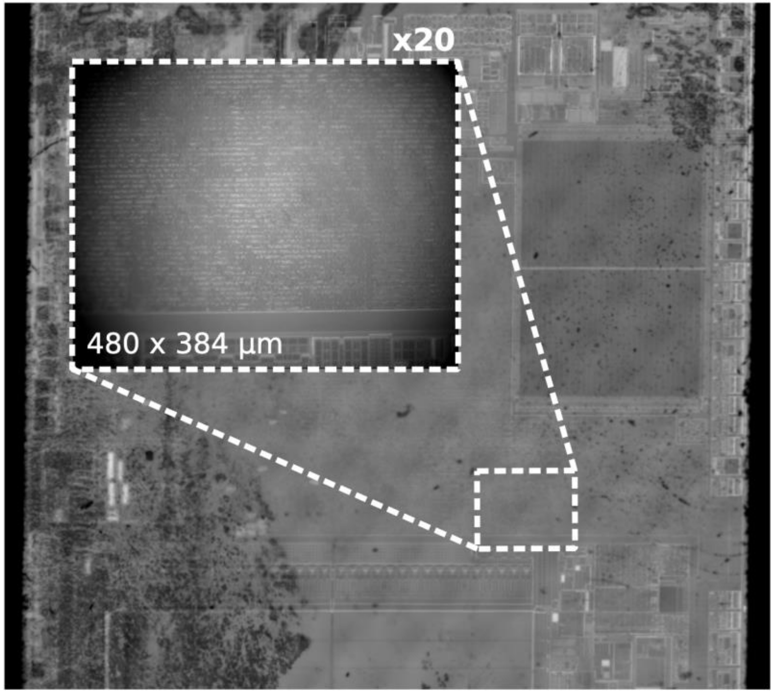


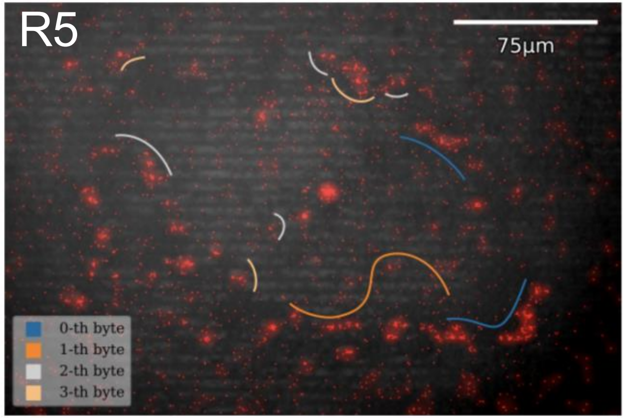
Pico-second laser source: 60 ps pulses

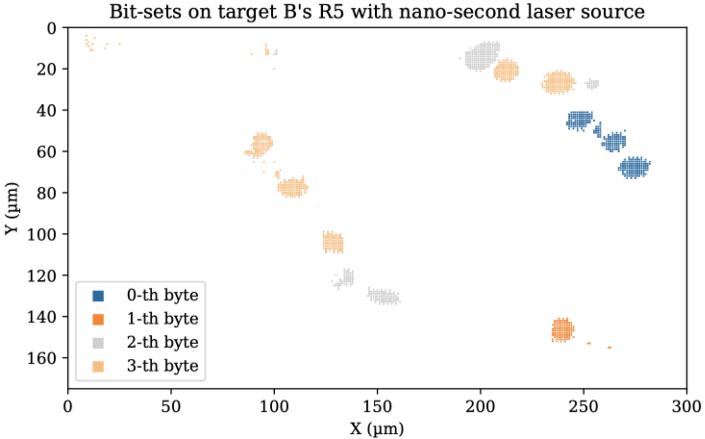
- ✓ 1,064 nm
- ✓ 0.12 nJ

PEM for LFI facilitation – More results

Target 2 – 32-bit ARM Cortex M0+, CMOS 90 nm







Betrayed by light – Using PEM as an Enabler of LFI

- Photon Emission (PE) basics
- PEM setup and imaging methodology
- PEM for LFI facilitation

- Conclusion

Betrayed by light – Using PEM as an Enabler of LFI

- Conclusion – PEM
  - ✓ Efficient reverse engineering of MCUs
  - ✓ Constraints
    - ✓ Backside, NIR imaging
    - ✓ Long integration times (code loops)
  - ✓ Integration into LFI setup
  - ✓ Mapping of CPU core registers + successful LFI

European Cyber Week

THE SOVEREIGN CYBER & DEFENCE AI FORUM

Contact:
dutertre@emse.fr

Betrayed by Light: How Photon Emission Microscopy Empowers Register Bit-level Laser Attacks on Microcontrollers, HOST 2025

H.Perrin, J.-M. Dutertre, J.B. Rigaud

Institut Mines-Télécom

Equipe Commune Systèmes et Architectures Sécurisées
Mines Saint-Etienne, CEA, Leti, Centre CMP
13541 Gardanne FRANCE