Hardware Reverse Engineering Workshop (HARRIS 2025)
17.-18. March 2025 Bochum, Germany

Data Extraction from Memory using Photon Emission Microscopy

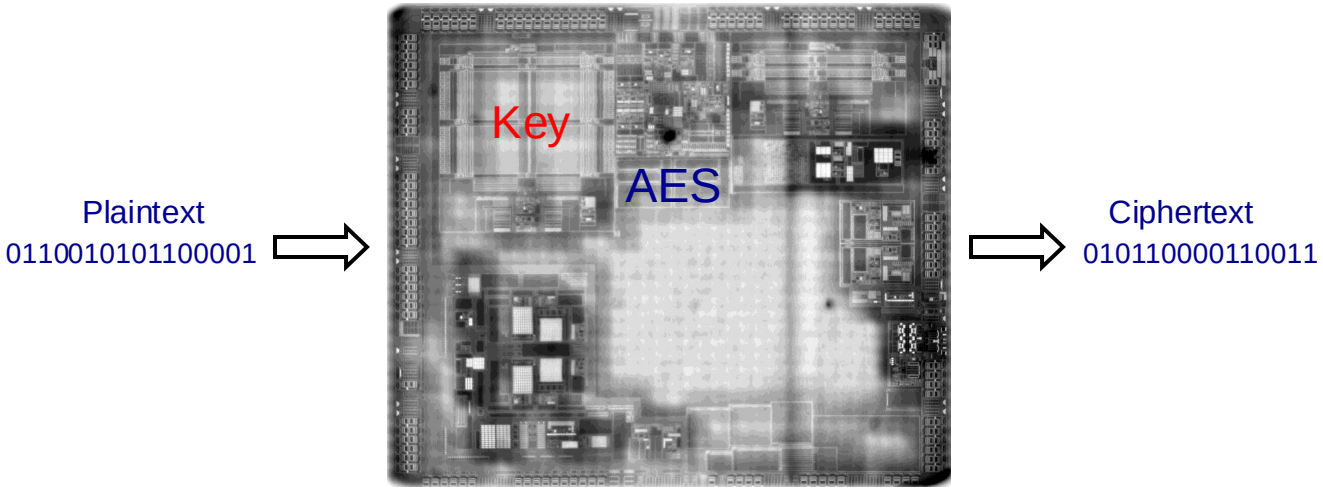
R. Silva Lima[1, 2], R. Viera[1], J.-M. Dutertre[1], W. Magrini[2], M. Pommies[2], A. Bertrand[2]

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

(2) Centre Technologique ALPhANOV – Systèmes Optiques

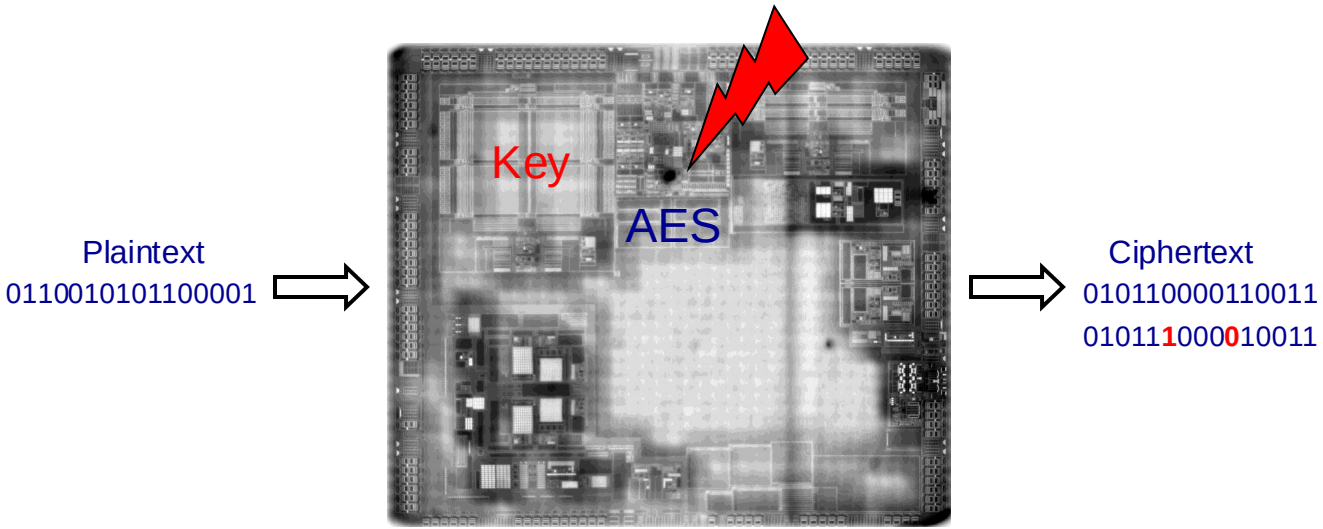
Context – Hardware security

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



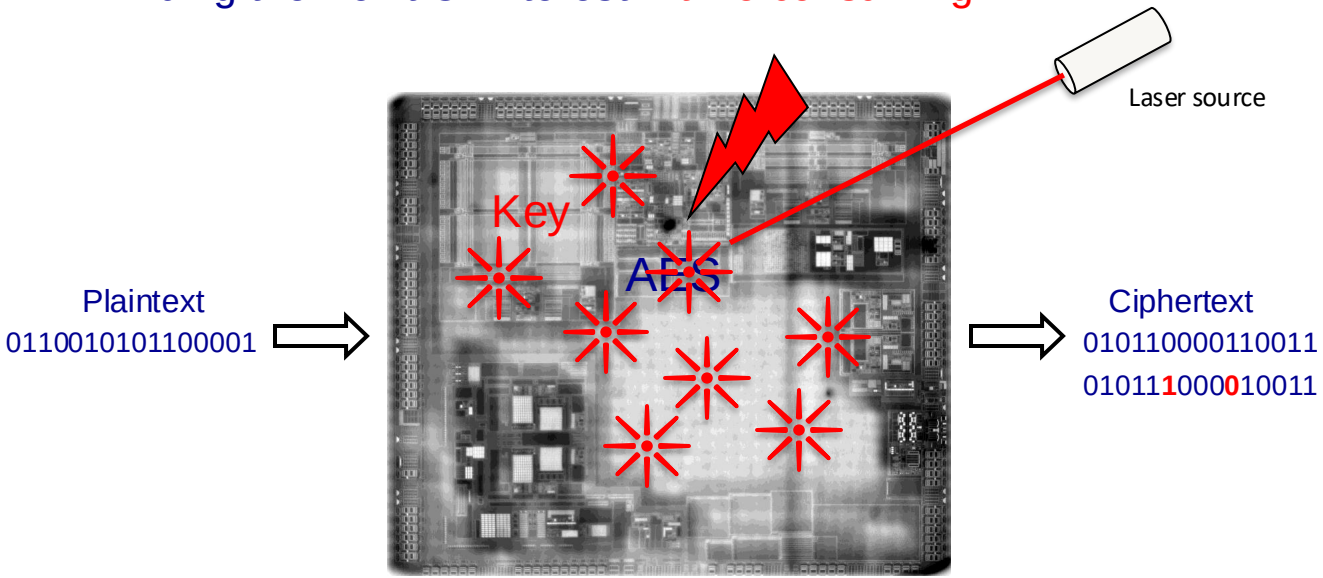
Context – Hardware security

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



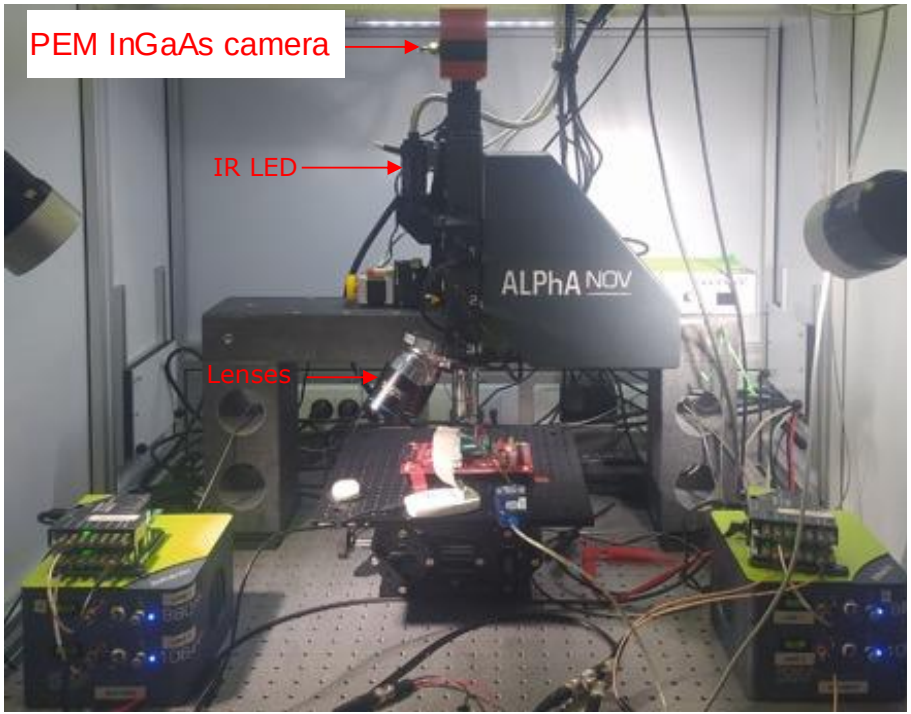
Context – Hardware security

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



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

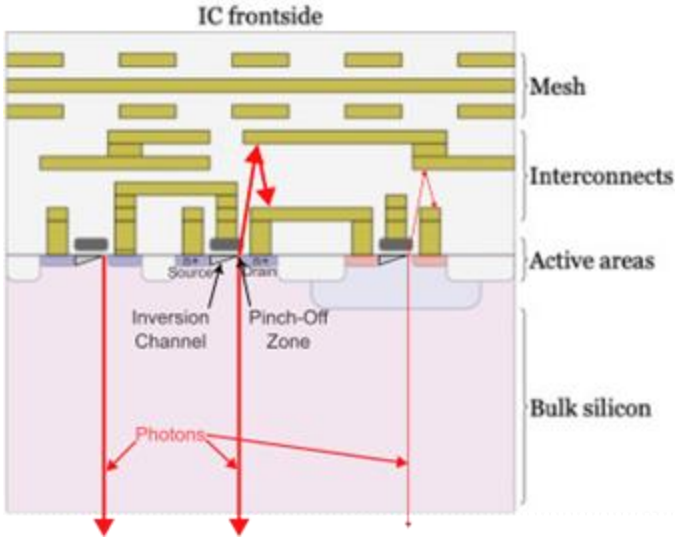
- Q? Data leakage/extraction?

Data Extraction from Memory using PEM

- Photon Emission (PE) basics
- Data extraction from SRAM memories
  - ✓ Memory organization
  - ✓ PEM at read and write time
  - ✓ PE from read/write logic
- Data extraction from Flash memories
  - ✓ Flash modes of operation
  - ✓ PEM at erase and program time
  - ✓ Data dependency of PE
- From limitations to a practical attack scenario

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)
  - ✓ $NMOS_{emission} > PMOS_{emission}$



[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

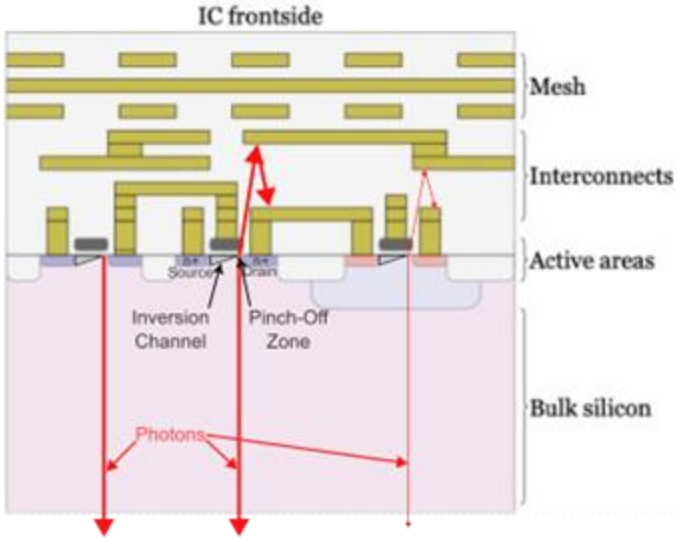
Backside PEA (λ= 1-2 µm)

(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]

Photon Emission Microscopy (PEM) setup

Photon Emission maps → transistors activity maps

Camera:

- ✓ 640x512 InGaAs sensor
- ✓ On a LFI bench

- ✓ Typical readout noise (rms) : 18 e^-
- ✓ Typical dark current (@-15 °C) : < 750 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

On a running device

→ execution of code loops

⇨ Strong constraints for attack purposes

→ white box model:

- ✓ Ability to execute arbitrary code loops
- ✓ Synchronization

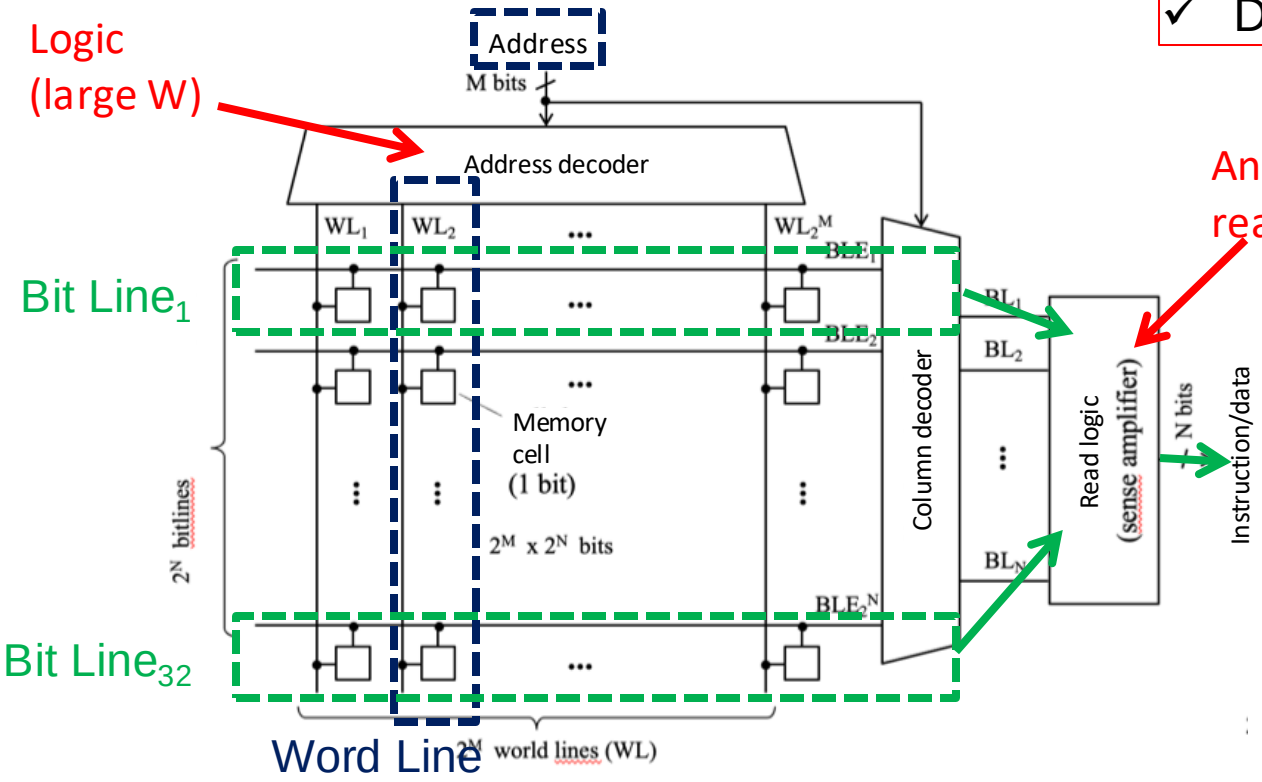
Data Extraction from Memory using PEM

- Photon Emission (PE) basics
- Data extraction from SRAM memories
  - ✓ Memory organization
  - ✓ PEM at read and write time
  - ✓ PE from read/write logic
- Data extraction from Flash memories
  - ✓ Flash modes of operation
  - ✓ PEM at erase and program time
  - ✓ Data dependency of PE
- From limitations to a practical attack scenario

Memory organization

Attacker:
- ✓ Memory organization (RE)
- ✓ Data extraction

Main photon emitters

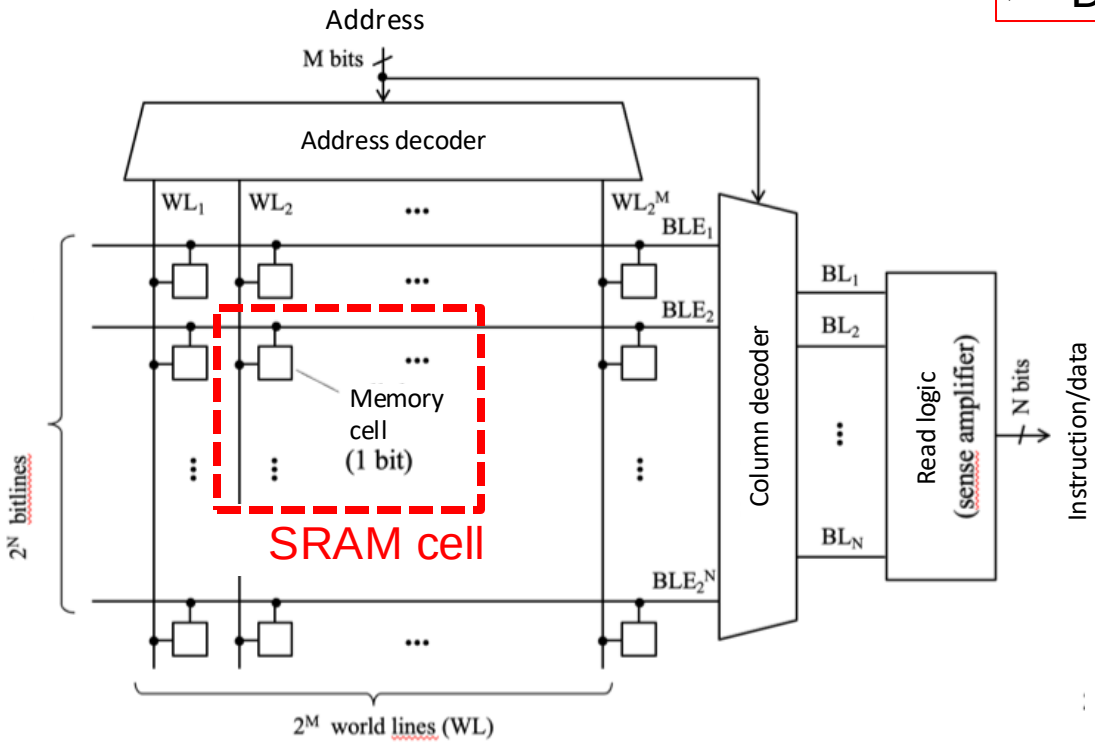


Memory organization

Attacker:

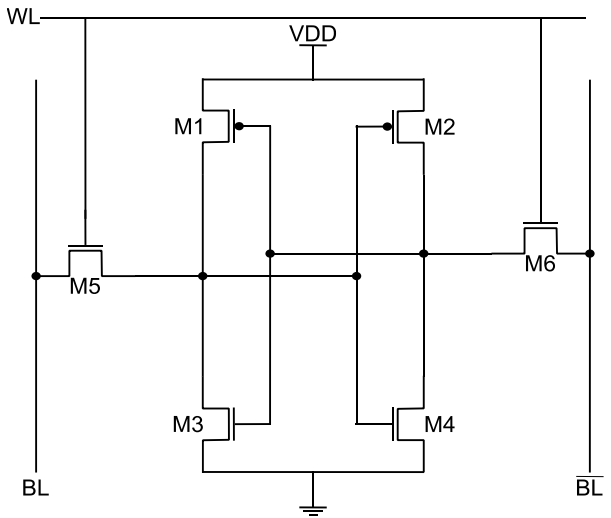
- ✓ Memory organization (RE)
- ✓ Data extraction

Main photon emitters



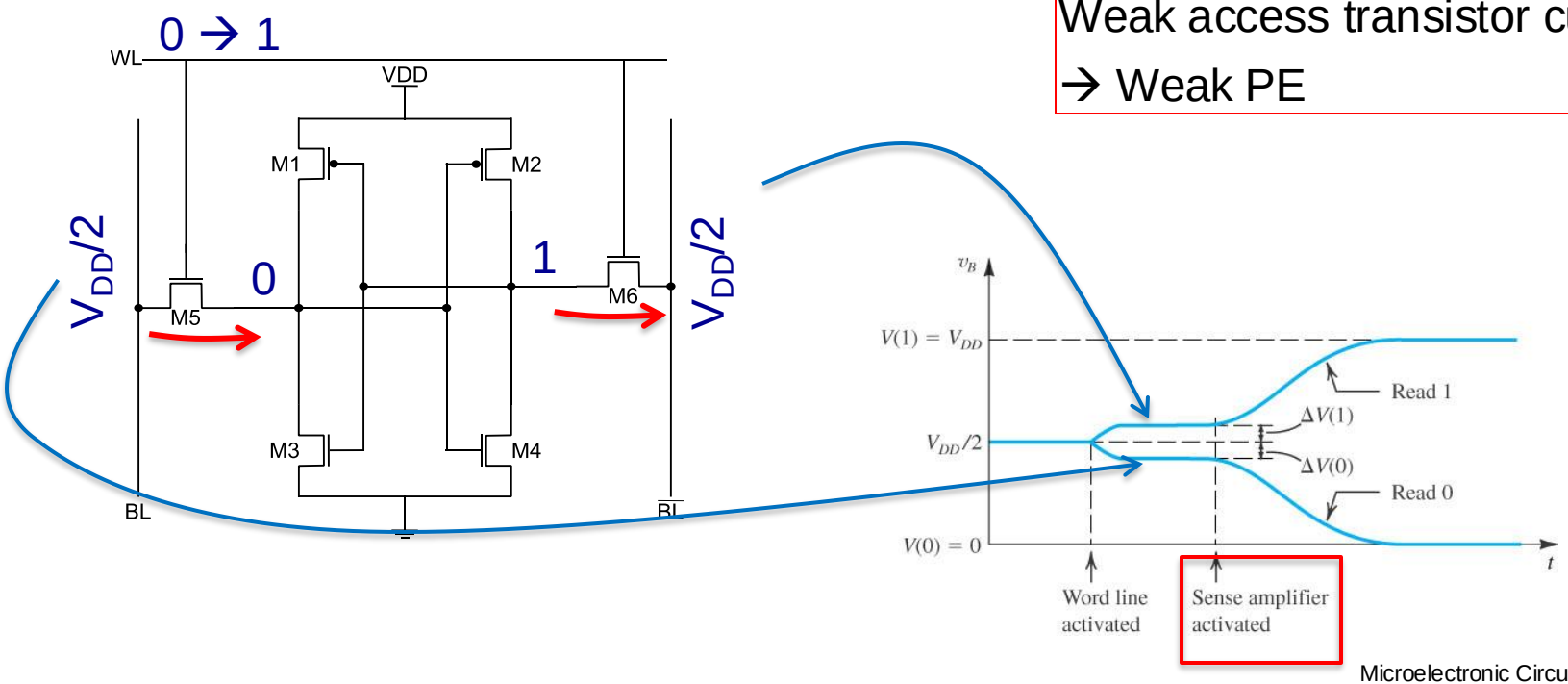
SRAM photon emission – Theory

6T SRAM cell



SRAM photon emission – Theory

6T SRAM cell – At read time



Weak access transistor current

→ Weak PE

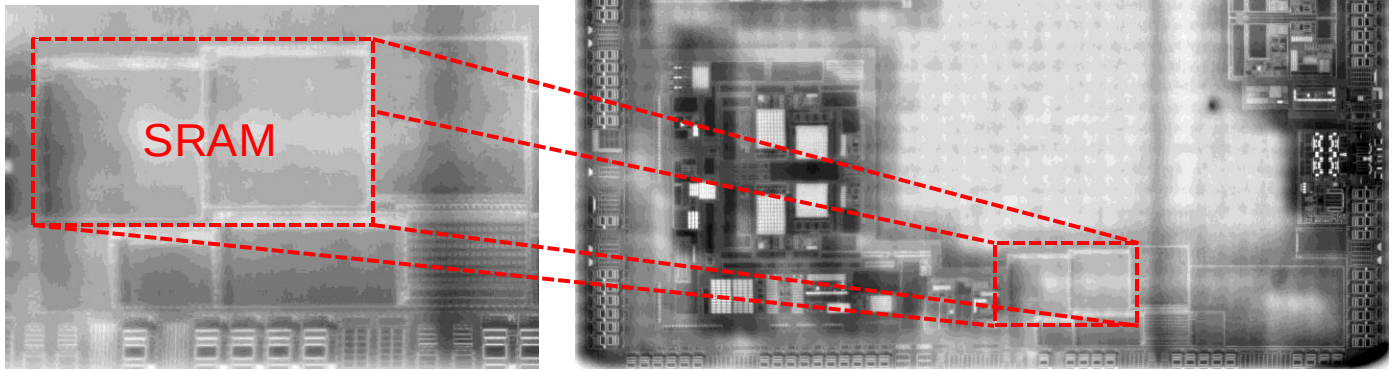
Microelectronic Circuits
Sedra/Smith

SRAM photon emission – Exp. results

Target 1 – At read time

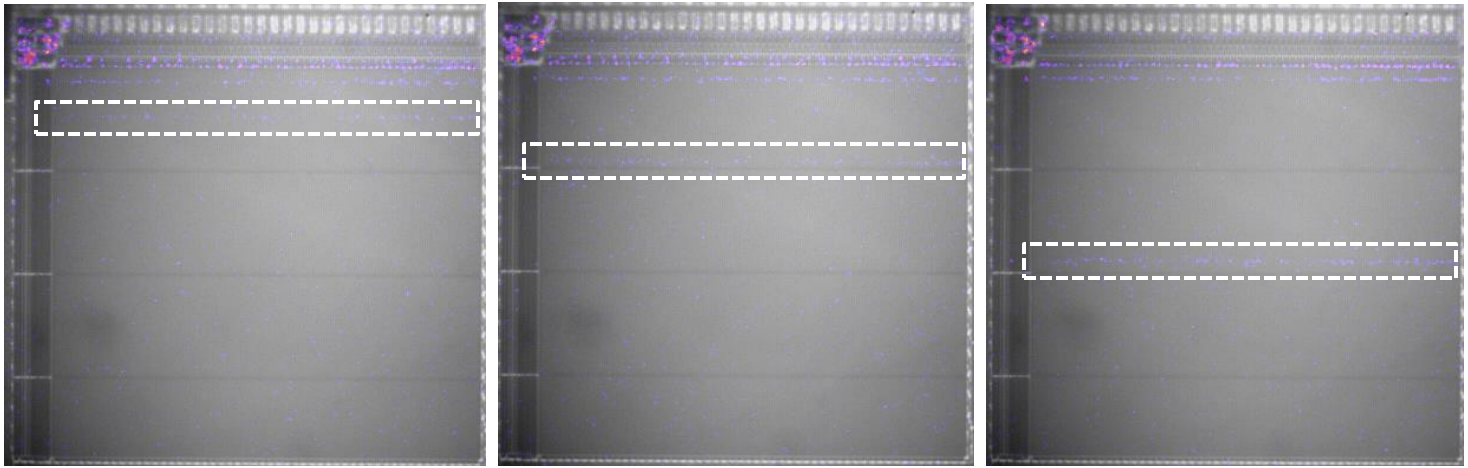
2x 16 kBytes SRAM

- ✓ Left even @
- ✓ Right odd @
- ✓ 0x20000000 – 0x20007FFF



SRAM photon emission – Exp. Results (read)

Target 1 – PE at read time



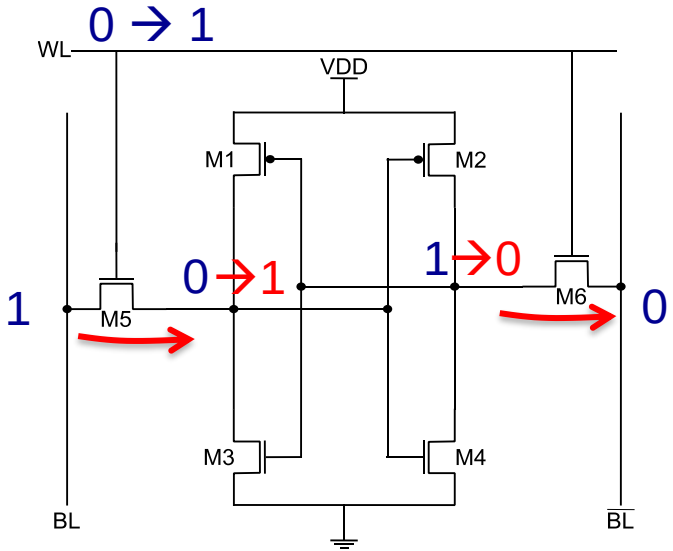
Photon emission map at read time: 20x lens, exposure 5s

@: 0x20001000 - 0x20003000 - 0x20004000 (left to right)

⇨ Weak emission at read time

SRAM photon emission – Theory

6T SRAM cell – At write time (0 → 1)



Switching inverters

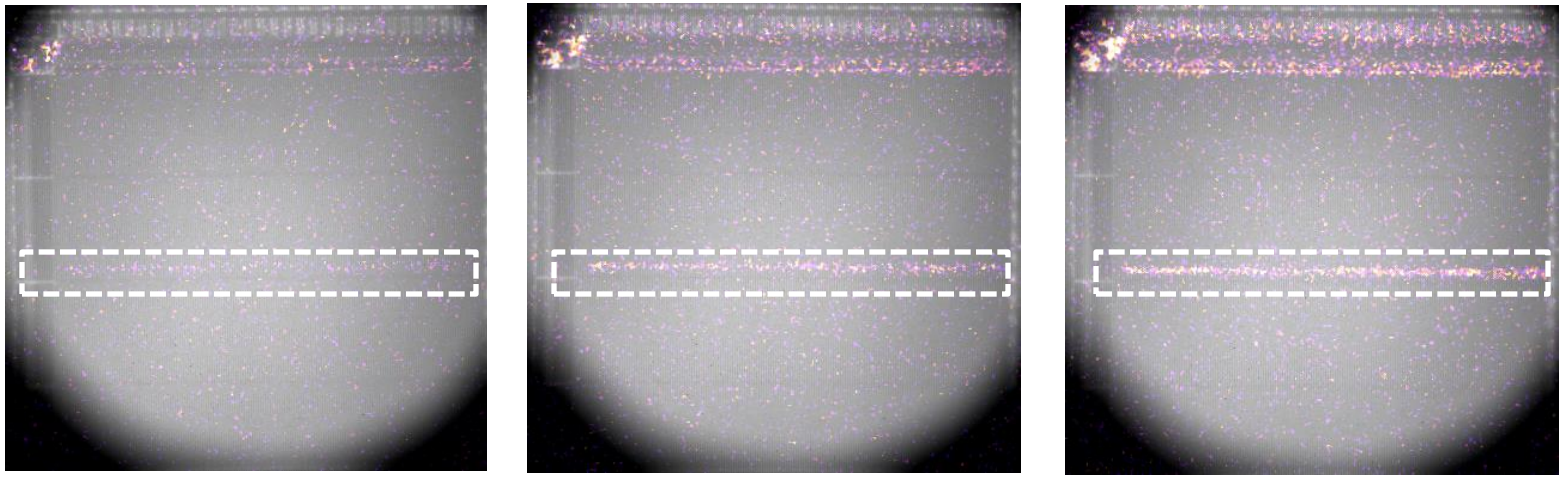
+ Strong access T current

→ Strong PE

SRAM photon emission – Exp. results (write)

Target 1 – PE at write time

Test code: write 0x00000000, then 0xFFFFFFFF



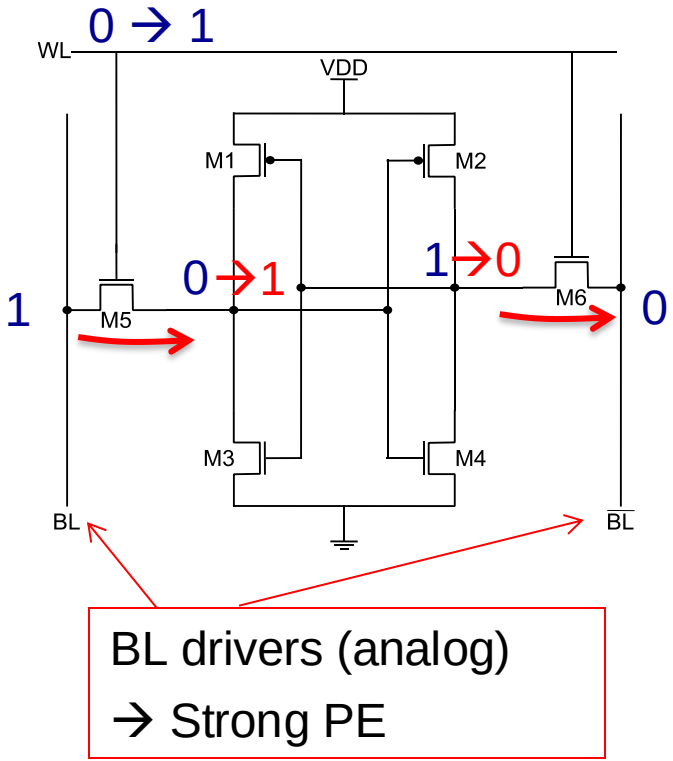
Photon emission map at write time: 20x lens, exposure 5s, @: 0x20004000

1 word, 8 words, 64 words (left to right)

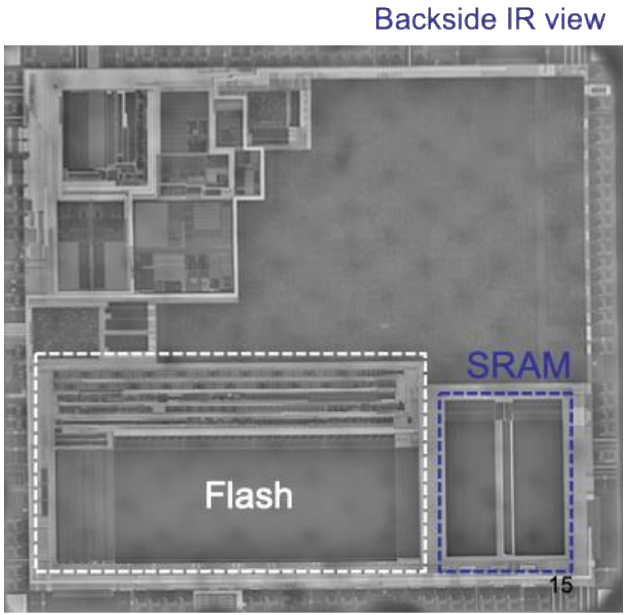
1 write cycle ~ 550ns → : 9.1 Mio. cycles in 5s

SRAM photon emission – Theory

6T SRAM cell – At write (read) time



Target 2



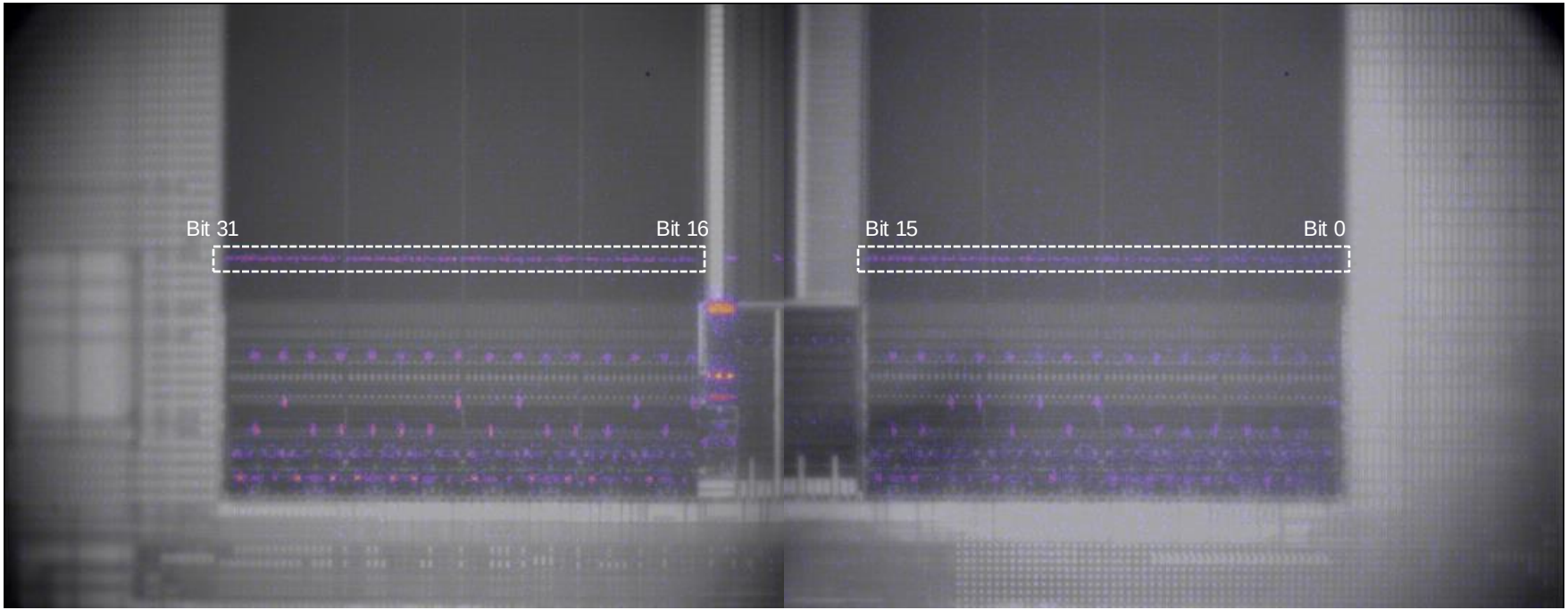
128 kBytes Flash 8 kBytes SRAM

✓ page size = 1 kB

SRAM data leakage – Exp. results

Target 2 – PE from read/write analog logic

Test code: write 0xBEBACAFE (loops)

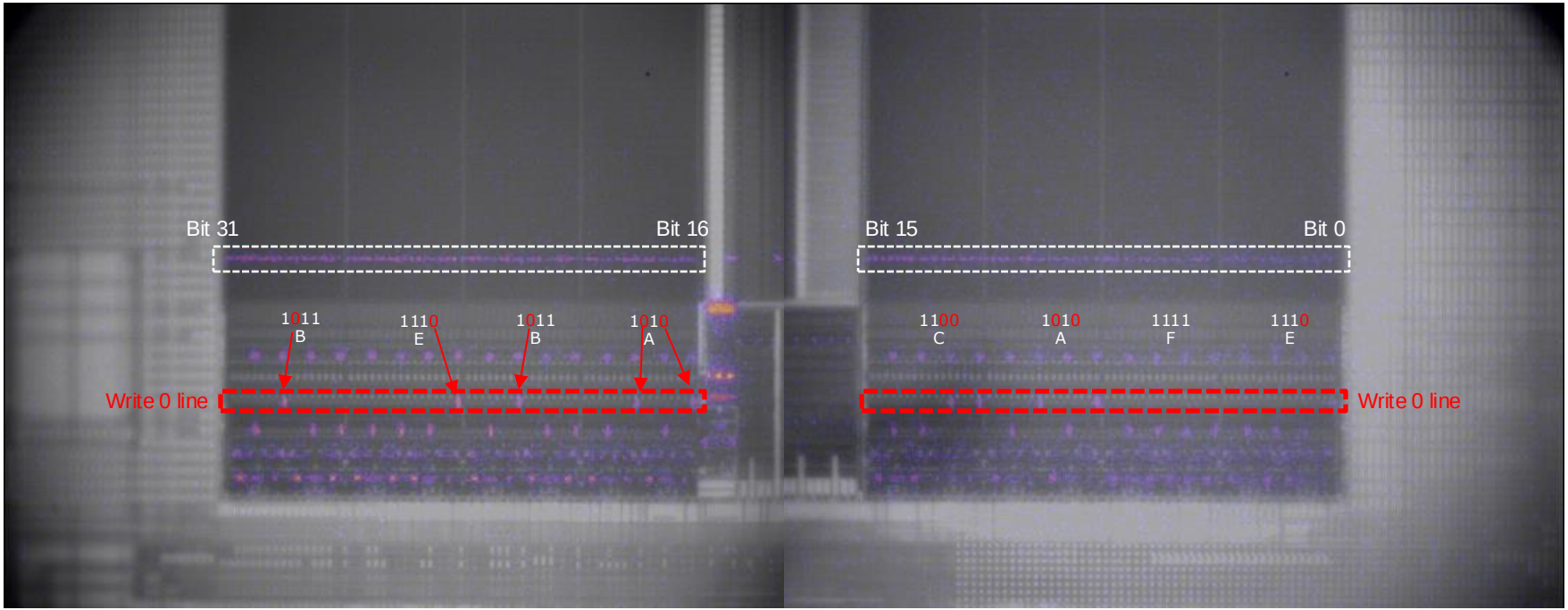


Photon emission map at write time: 20x lens, exposure 2.5s, 1 word

SRAM data leakage – Exp. results

Target 2 – PE from read/write analog logic

Test code: write 0xBEBACAFE (loops)

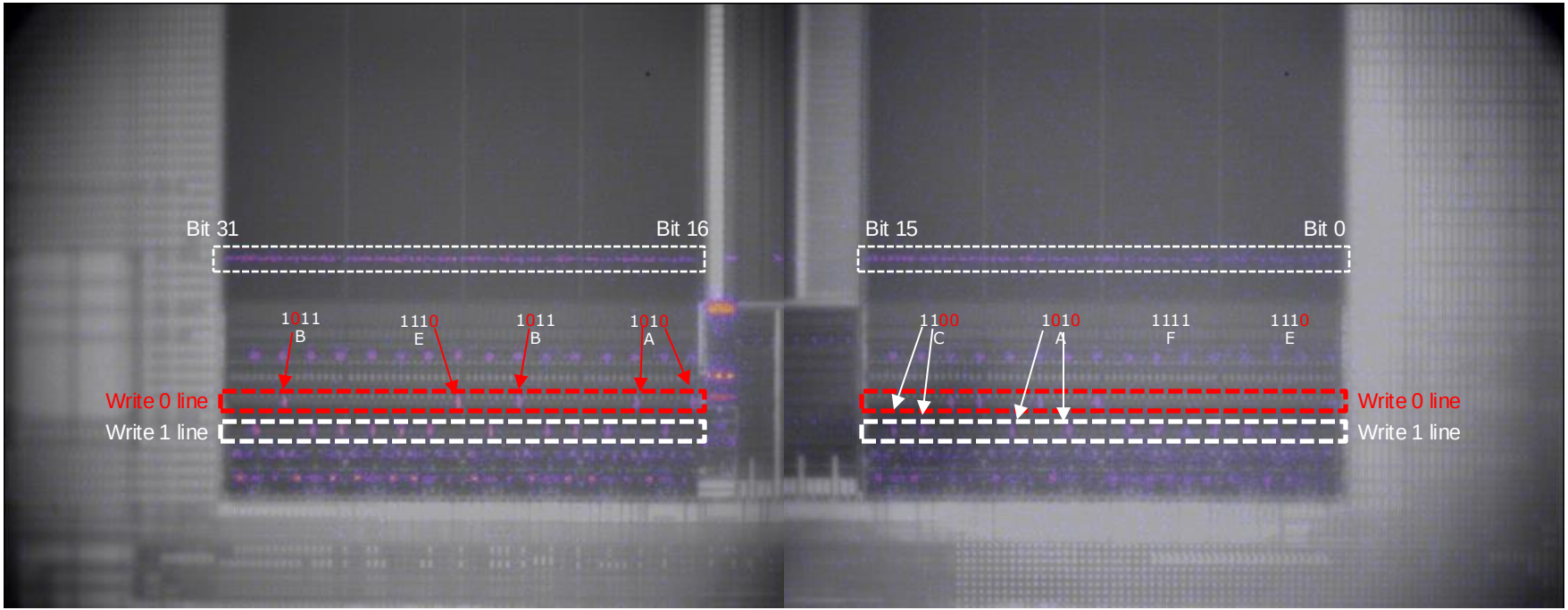


Photon emission map at write time: 20x lens, exposure 2.5s, 1 word

SRAM data leakage – Exp. results

Target 2 – PE from read/write analog logic

Test code: write 0xBEBACAFE (loops)

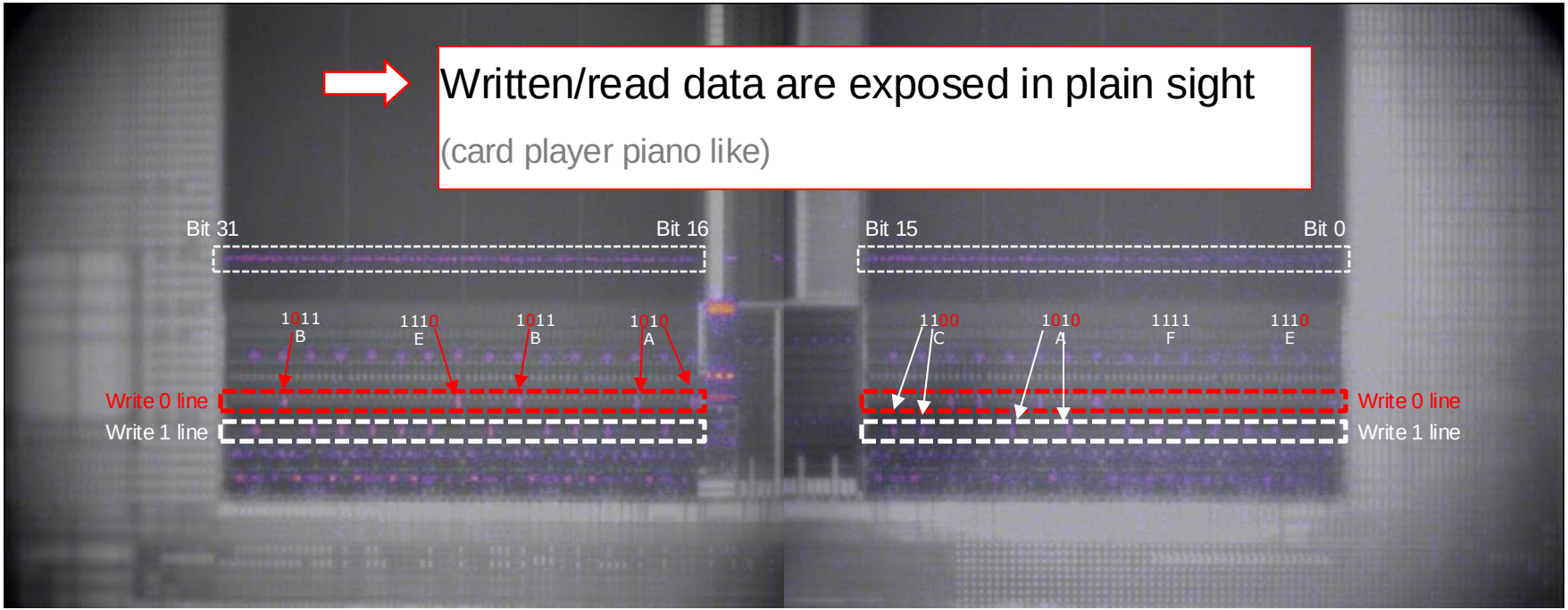


Photon emission map at write time: 20x lens, exposure 2.5s, 1 word

SRAM data leakage – Exp. results

Target 2 – PE from read/write analog logic

Test code: write 0xBEBACAFE (loops)



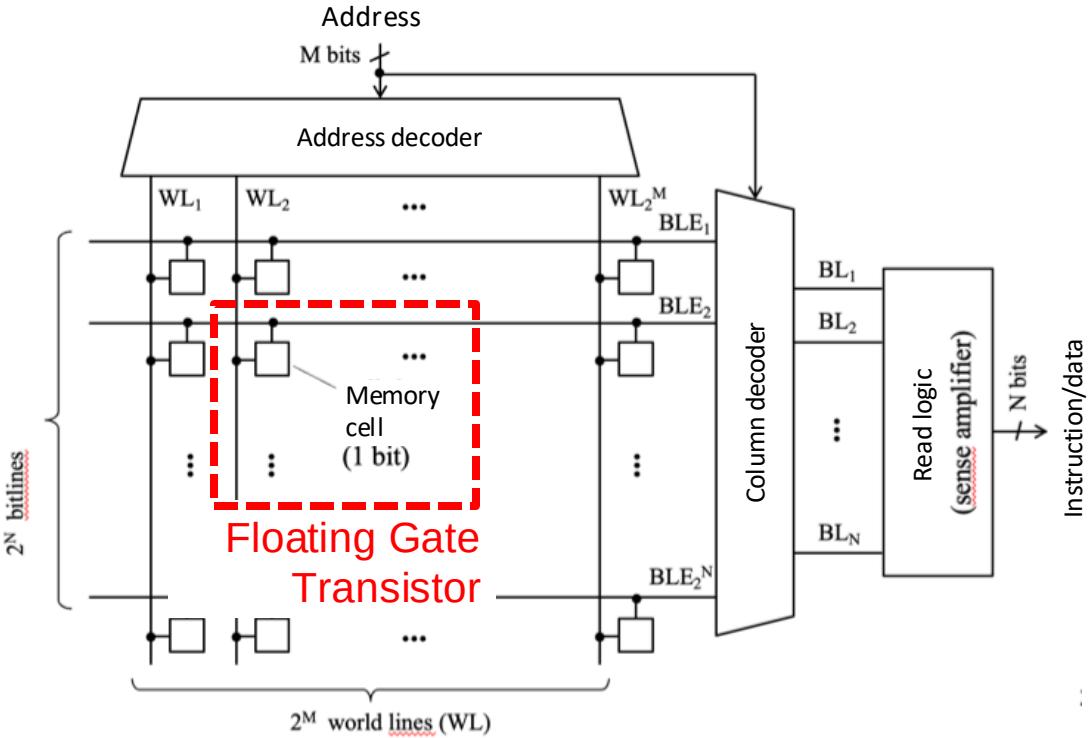
Photon emission map at write time: 20x lens, exposure 2.5s, 1 word

Data Extraction from Memory using PEM

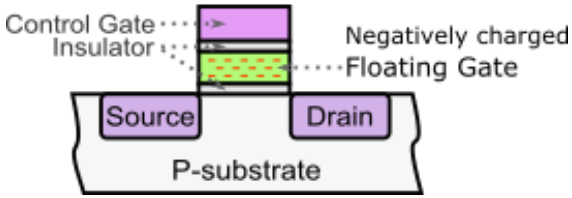
- Photon Emission (PE) basics
- Data extraction from SRAM memories
  - ✓ Memory organization
  - ✓ PEM at read and write time
  - ✓ PE from read/write logic
- Data extraction from Flash memories
  - ✓ Flash modes of operation
  - ✓ PEM at erase and program time
  - ✓ Data dependency of PE
- From limitations to a practical attack scenario

Flash memory organization

Unit cell: FG transistor



Flash memory modes of operation

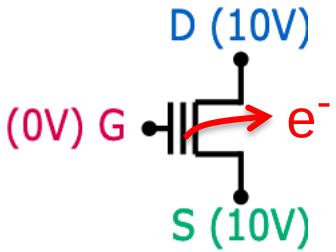


Writing in an embedded Flash is a complex 2-step process: erase & program

Flash memories are …

- ✓ … erased at page level (e.g. 1 kB)
- ✓ Fowler-Nordheim tunneling effect

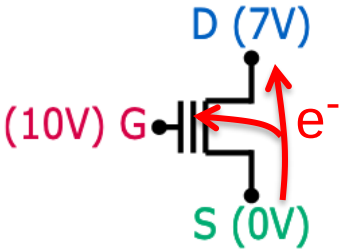
→ Set to 1 (or 0xFFFFFFFF at word level)



Erase

- ✓ … programmed (i.e. written) at word level
- ✓ Using channel-hot-electron injection

→ Set to 0 (or 0x00000000 at word level)

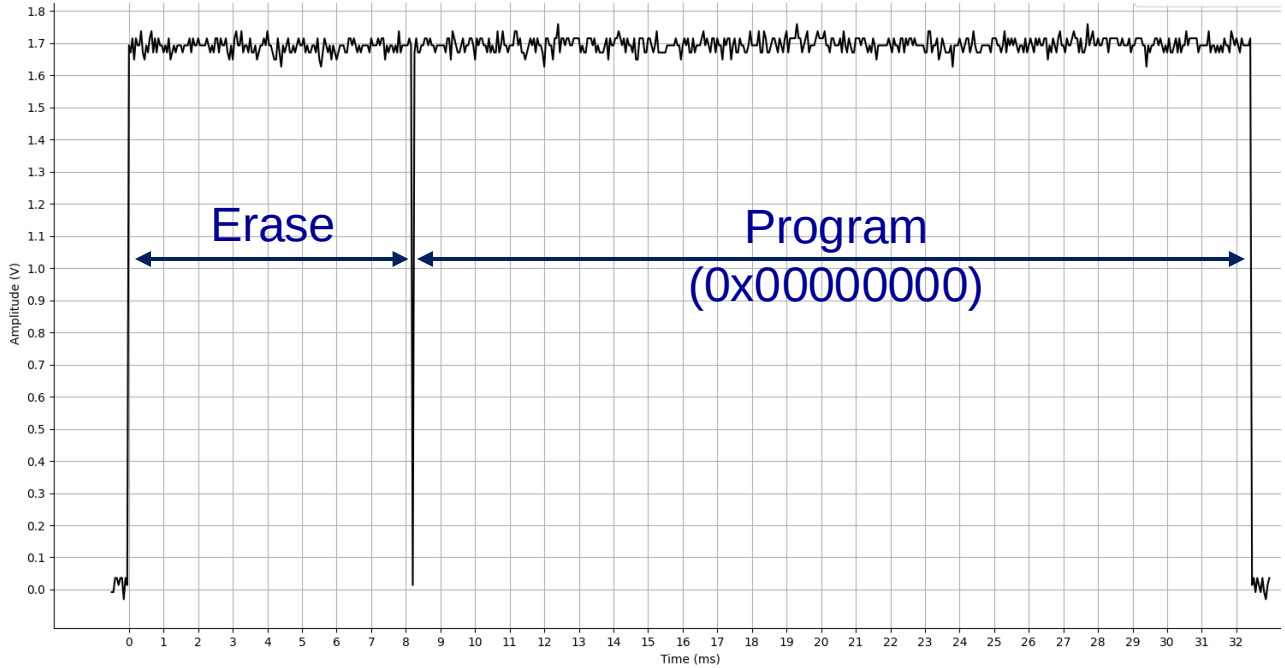


Program

Flash memory modes of operation

Erase + Program cycle time = 32 ms (32 cycles in 1 second)

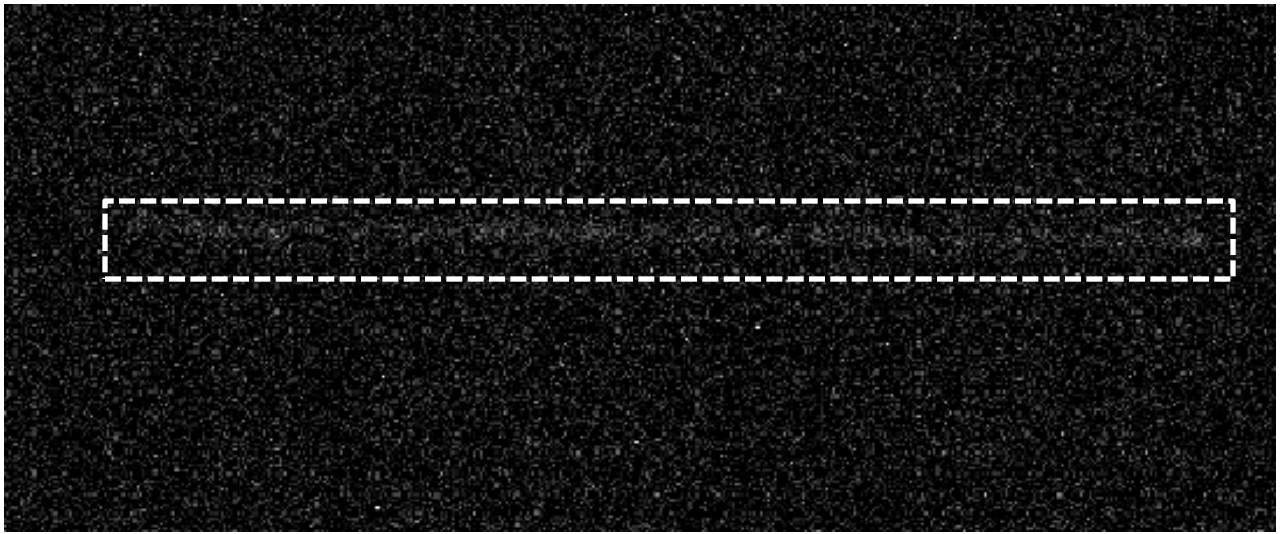
1 page



Flash photon emission – Exp. Results

Target 1 – erase + program

Number of erase + program cycles needed for the information to emerge from noise?

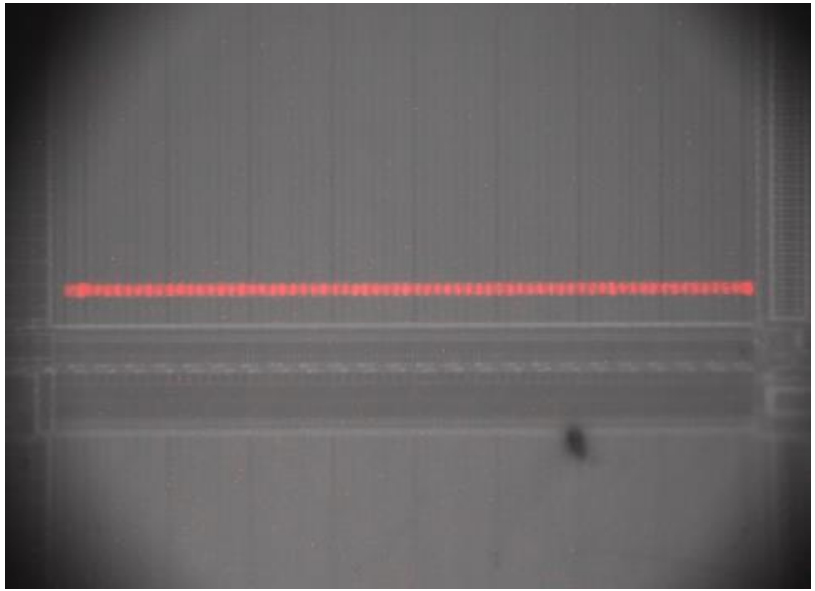


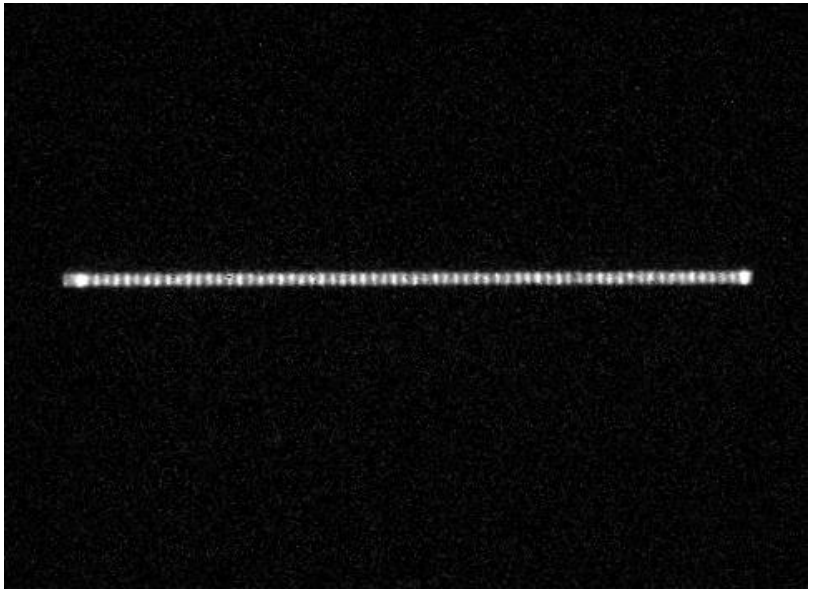
Photoemission map: 10 cycles, Page #255

Flash photon emission – Exp. Results

Target 1 – Data dependency

Target thinned down to 50 µm



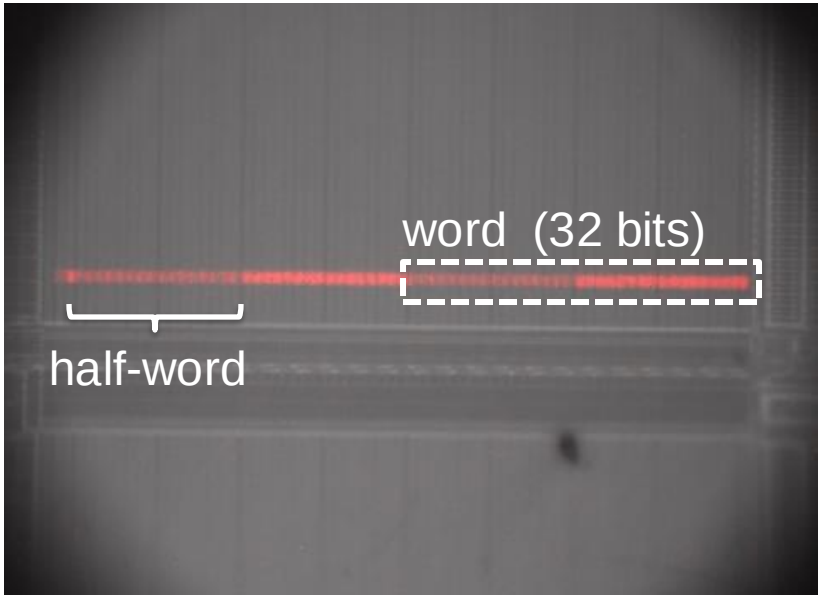


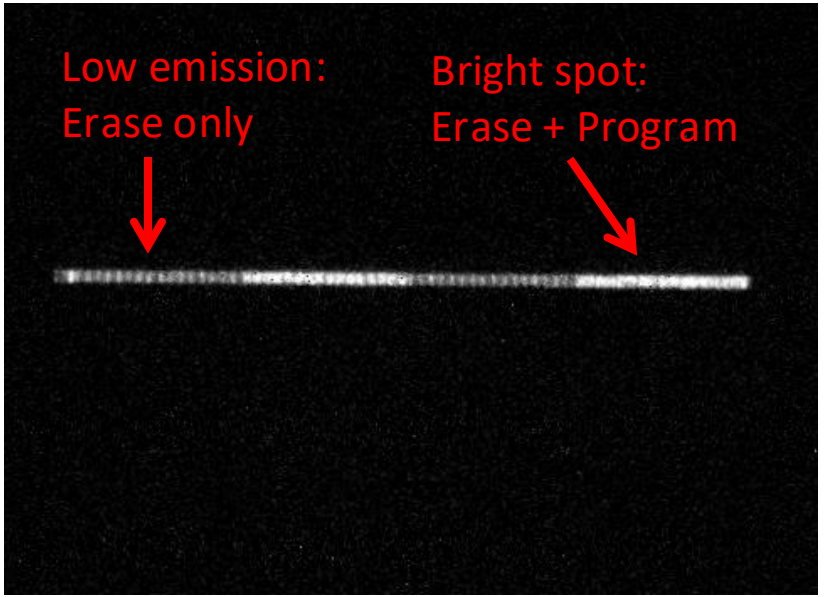
Page #120, 20x lens, exposure 2.5 s, program 0X00000000 (erase + program)
Overlay (left) & camera output (right)

Flash photon emission – Exp. Results

Target 1 – Data dependency

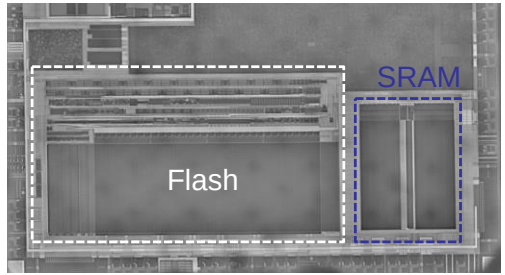
Target thinned down to 50 µm



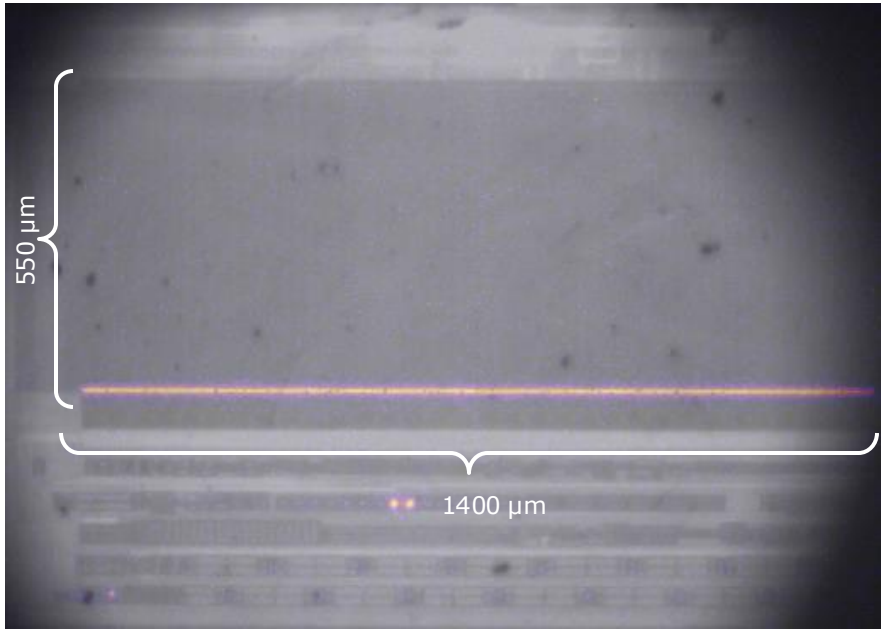


Page #120, 20x lens, exposure 2.5 s, program 0X0000FFFF

Flash photon emission – Exp. Results



Target 2 – Data dependency

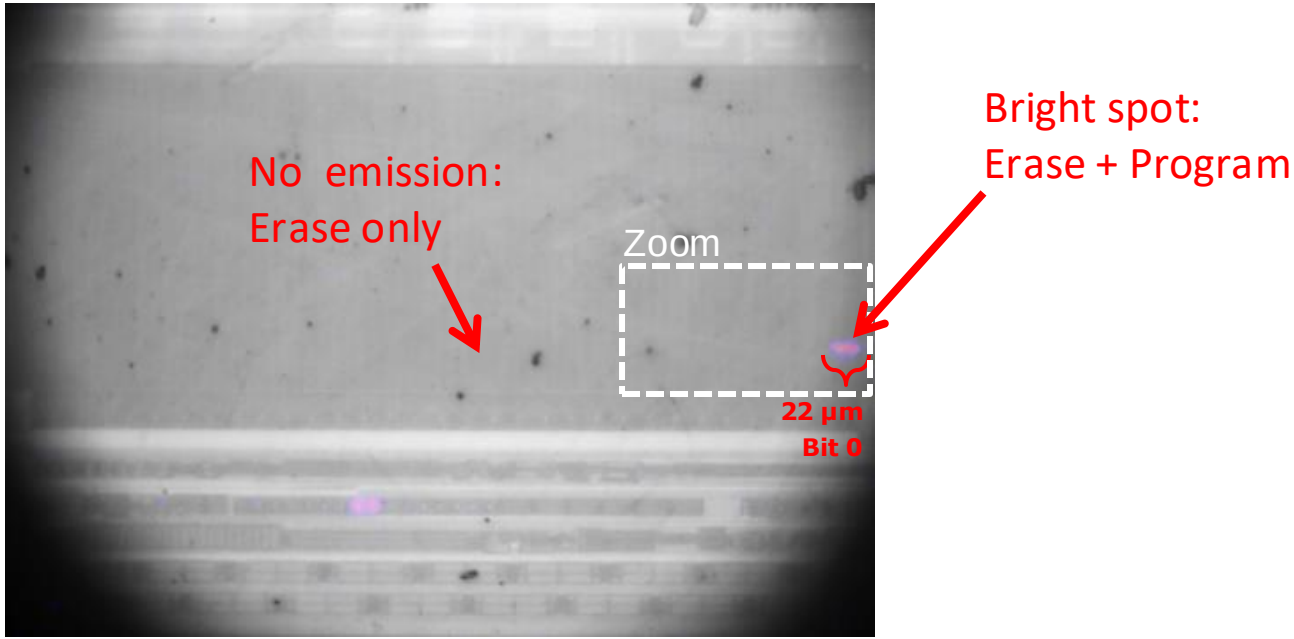


Page #127, 5x lens, exposure 2.5 s, program 0x00000000, 80 erase+prog. cycles

@: 0801FC00 – 0801FFFF

Flash photon emission – Exp. Results

Target 2 – Data dependency, Flash bits location

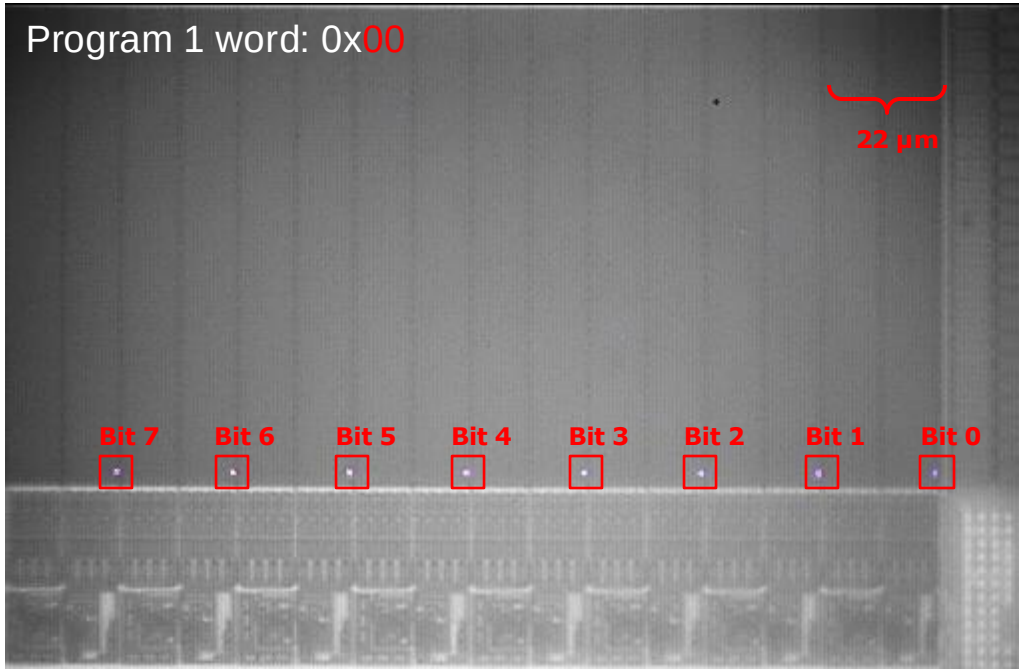


Page #127, 5x lens, exposure 2.5 s, program 0xFFFFFFFE, 80 erase+prog. cycles

@: 0801FC00 – 0801FFFF

Flash photon emission – Exp. Results

Target 2 – Data dependency, Flash bits location → lsb (programming a single word)

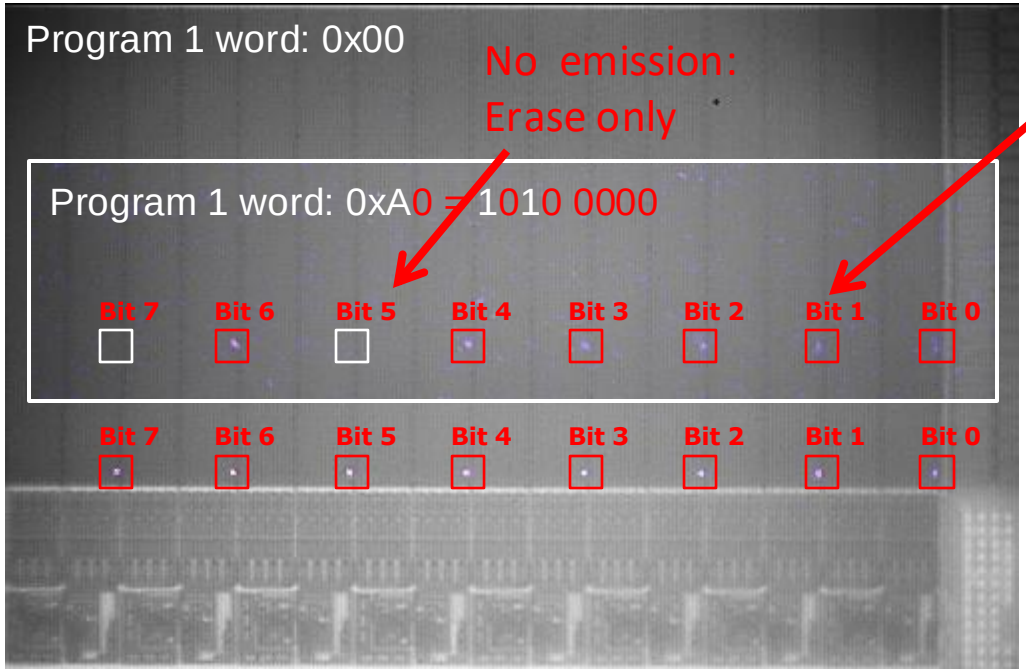


Page #127, 20x lens, exposure 2.5 s, program 0x00, 250 erase+prog. cycles

@: 0801FC00

Flash photon emission – Exp. Results

Target 2 – Data extraction at byte level



Bright spot:
Erase + Program

Page #127, 20x lens, exposure 2.5 s, program 0x00, 250 erase+prog. cycles

@: 0801FC00

Data Extraction from Memory using PEM

- Photon Emission (PE) basics
- Data extraction from SRAM memories
  - ✓ Memory organization
  - ✓ PEM at read and write time
  - ✓ PE from read/write logic
- Data extraction from Flash memories
  - ✓ Flash modes of operation
  - ✓ PEM at erase and program time
  - ✓ Data dependency of PE
- From limitations to a practical attack scenario

Practical attack scenario

Taking advantage of Flash modes of operation

✓ Page-level erase

Password identification routine

✓ Admin password (secret) stored in Flash memory

✓ User password stored in the same Flash page

✓ The user can update his own password → initiate a erase + program cycle

Data extraction attack

The user updates (continuously) his password → loops

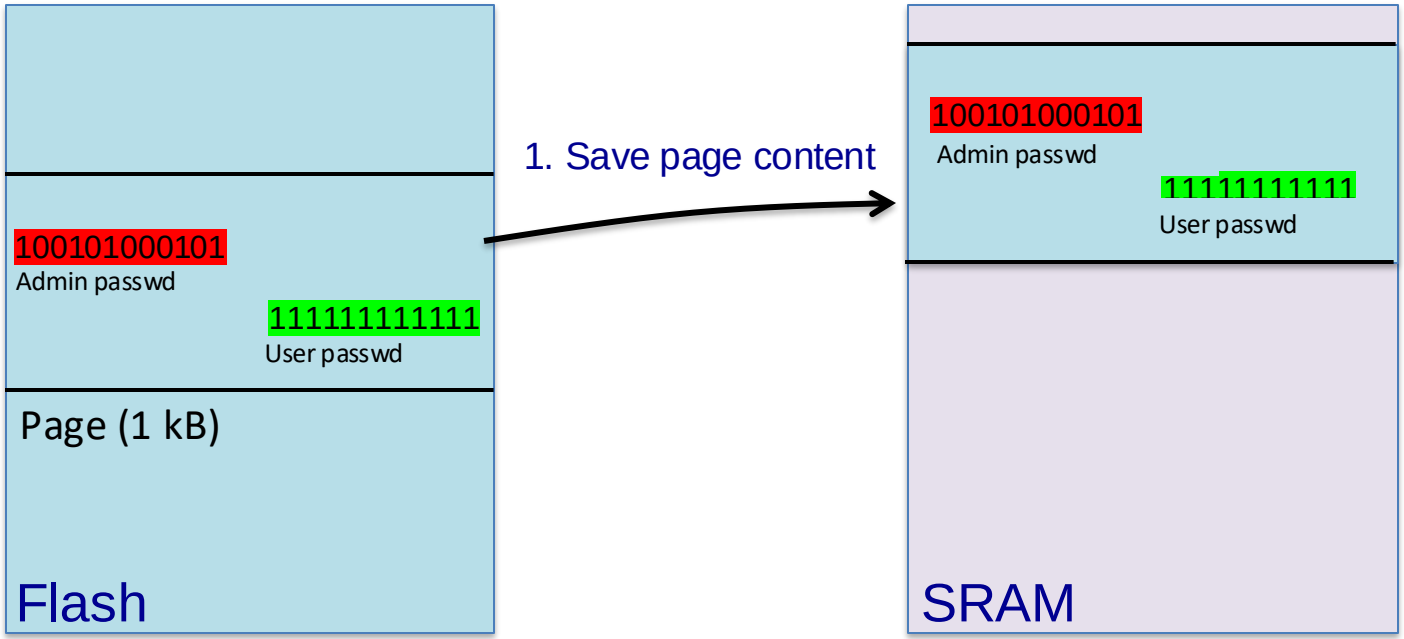
✓ Admin passwd stored in RAM

✓ Admin passwd written back in Flash → a erase + program cycle

Practical attack scenario

User password update

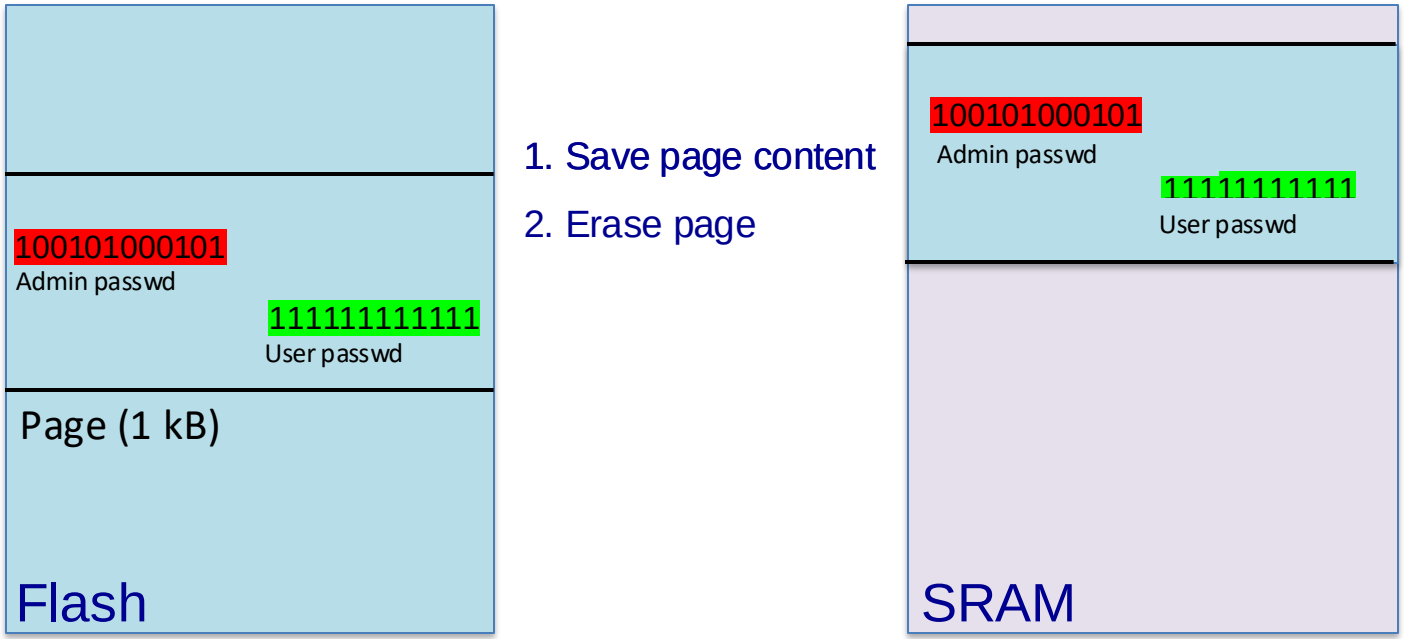
Flash Write → Erase (page-level) + Program



Practical attack scenario

User password update

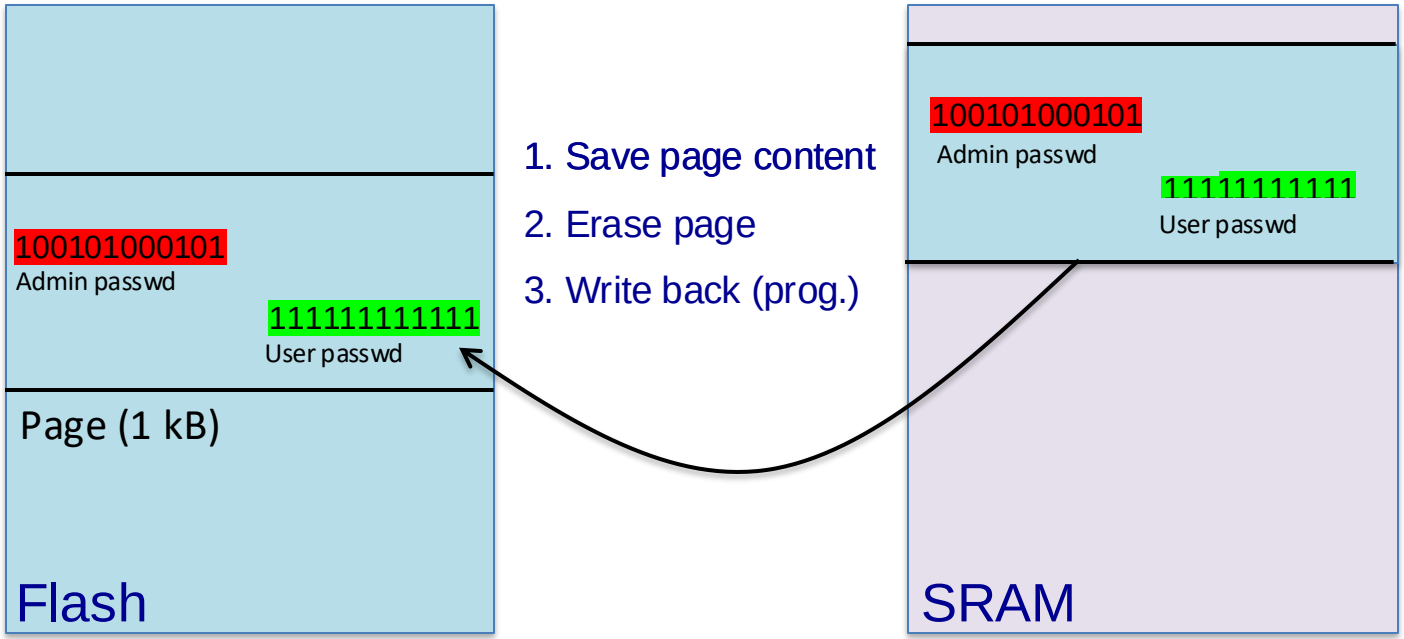
Flash Write → Erase (page-level) + Program



Practical attack scenario

User password update

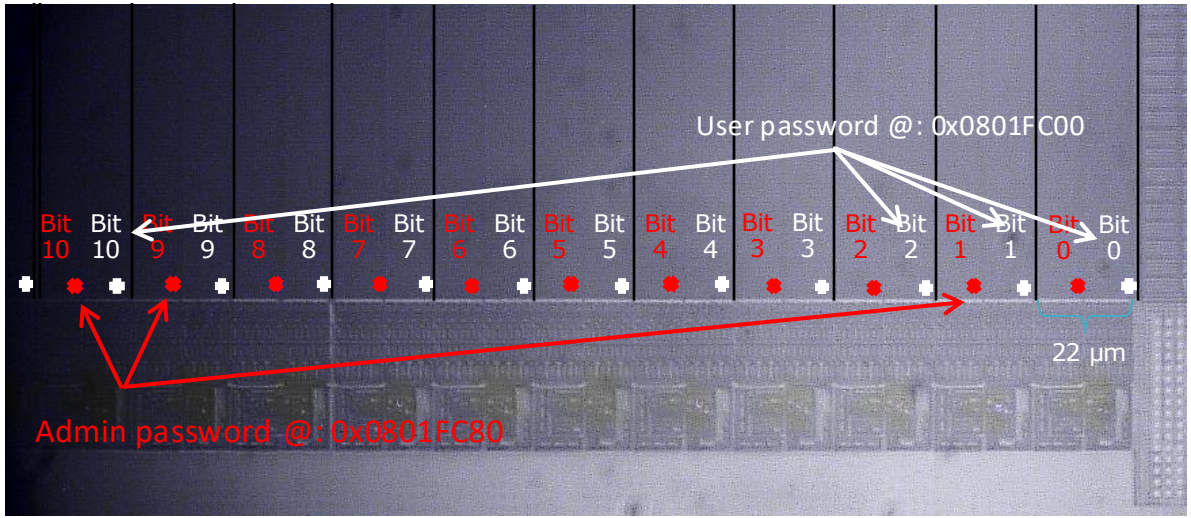
Flash Write → Erase (page-level) + Program



Flash att. scenario – Password extraction

Experimental results

- ✓ Admin password: 0xBEBACAFE, @: 0x0801FC80
- ✓ User password: 0xFFFFFFFE, @: 0x0801FC00

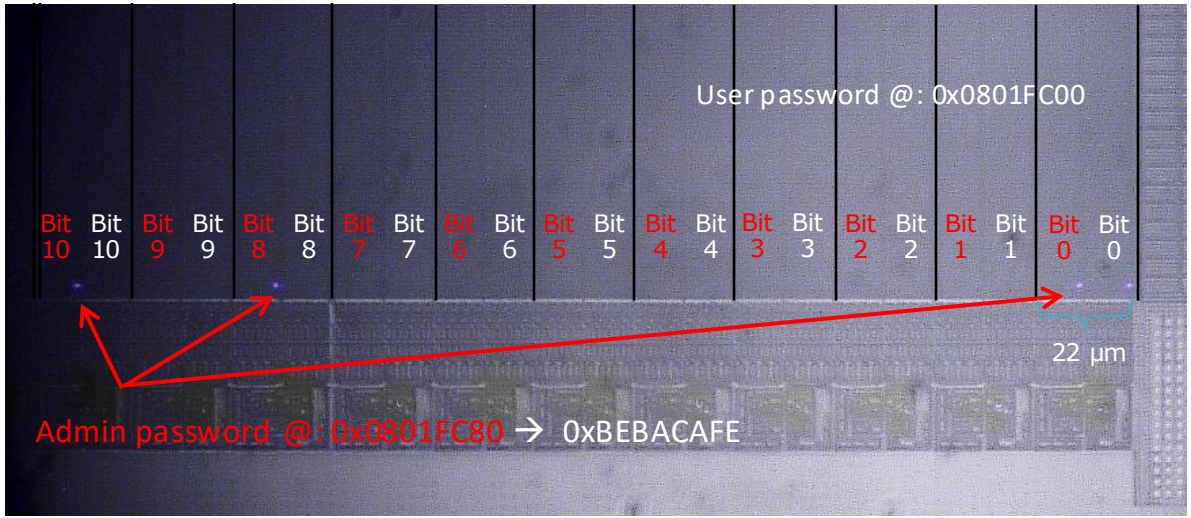


Photon emission map: 20x lens, exposure 100 s

Flash att. scenario – Password extraction

Experimental results

- ✓ Admin password: 0xBEBACAFE, @: 0x0801FC80
- ✓ User password: 0xFFFFFFFE, @: 0x0801FC00



Photon emission map: 20x lens, exposure 100 s

Conclusion

PEM reverse engineering capabilities

- ✓ Flash/SRAM architecture: WL, BL, bit cells (**Write** or read)
- ✓ Analog blocks → data extraction

PEM constraints

- ✓ Execution of code loops → not consistent with an attack scenario

⇨ Data extraction from memory at read/write time

Scaling → analog blocks are strong emitters of photons (adv. tech.)

Practical attack scenarios do exist

Contact:
dutertre@emse.fr

To go further:

- ✓ R.S. Lima et al., When data shines - leaking data from microcontrollers through photon emission analysis, ASHES 2024
- ✓ R. S. Lima et al., Reverse-engineering and data extraction from SRAM using photon emission analysis, IEEE PAINE 2024

MINES Saint-Étienne | Institut Mines-Télécom | ALPhA NOV Centre Technologique Optique et Lasers

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

Centre Technologique ALPhANOV – Systèmes Optiques