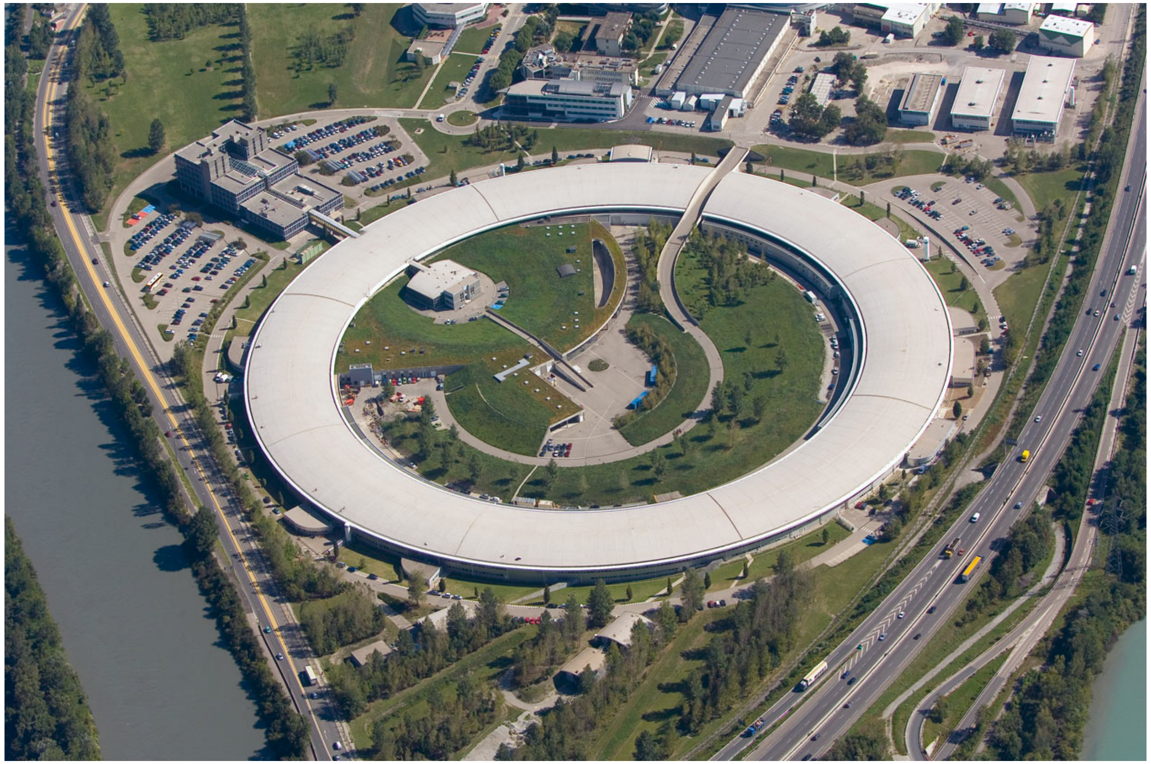
X-RAY A NEW WAY TO ATTACK / MODIFY INTEGRATED CIRCUITS

ANCEAU Stéphanie (CESTI)
BLEUET Pierre (LETI)
CLEDIERE Jessy (CESTI)
MAINGAULT Laurent (CESTI)
RAINARD Jean-Luc (CESTI)
TUCOULOU Rémi (ESRF)

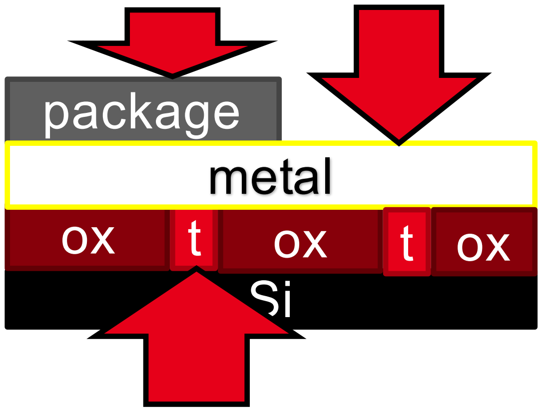
FROM RESEARCH TO INDUSTRY



X-RAYS : A BETTER LASER ?

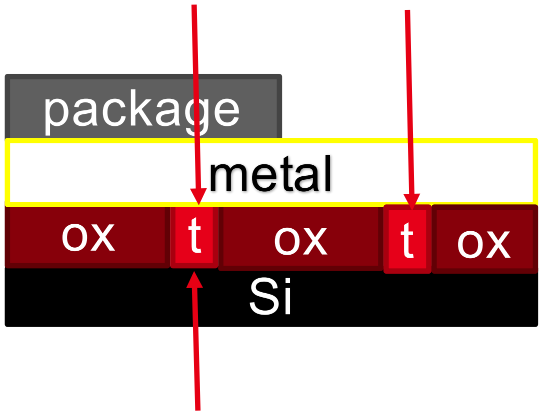
Laser perturbation (VIS-IR)

- Resolution limited by its wavelength (IR ~ 1 µm)
- Semi-invasive : Unpackage the device / bakside illumination



X (~ 10 keV)

- Wavelenght < 1 nm
- Non invasive : Package, thin metal layers → ~transparent

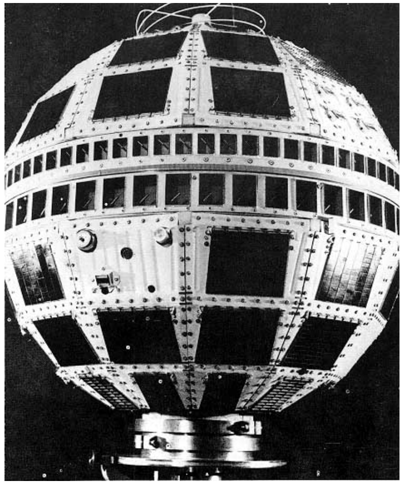


Litterature on fault injection with X-rays ?

Only in spatial (nuclear / medical imaging) articles

FIRST FAULTS ON ELECTRONIC CIRCUITS WITH IONIZING RADIATION

- Telstar 1962 : first communication satellite failed after atmospheric nuclear bomb tests



- From previous workshop : 1967' fault simulator

412 IEEE TRANSACTIONS ON ELECTRONIC COMPUTERS, VOL. EC-16, NO. 4, AUGUST 1967

Design and Use of Fault Simulation for Saturn Computer Design

FRED H. HARDIE AND ROBERT J. SUHOCKI

Why nothing in fault injection ?

1. Difficult to synchronize → Begin with memories (NVM + RAM)

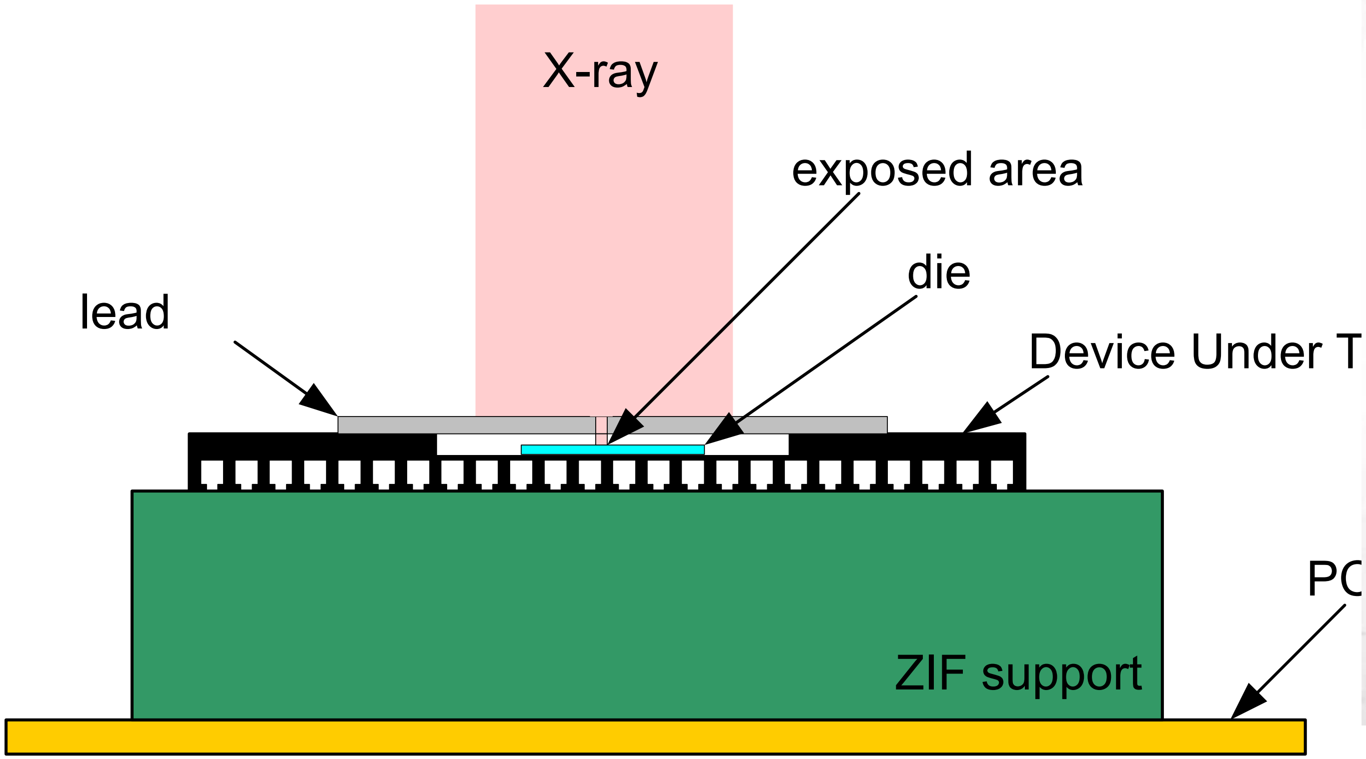
2. Hard to focus → Next slides

BASIC FOCUSING

w/h generic X-ray generator

…a hole in a lead sheet in FLASH mem

+ old component .35 µm (ATMega)



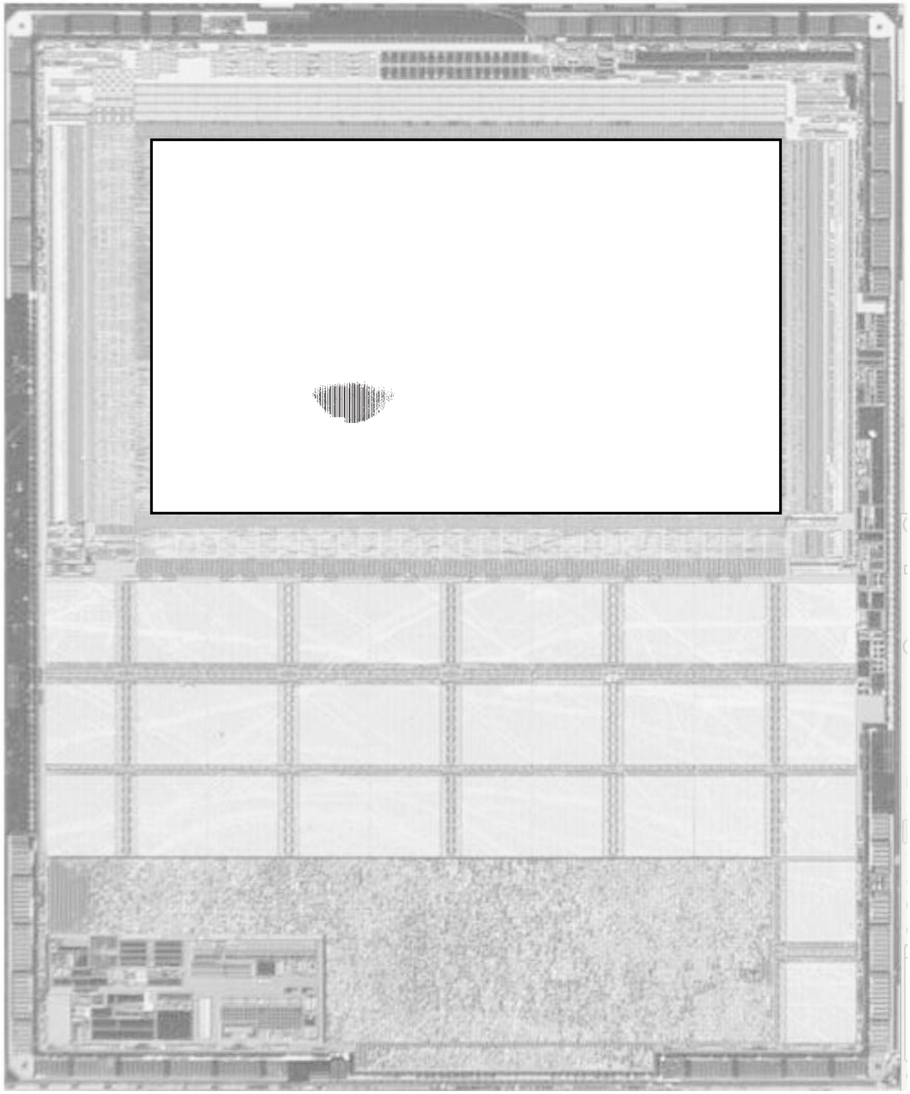
ATMEGA + lead sheet and hole

Flash memory filled with value *0x*AA

Exposure to X-rays

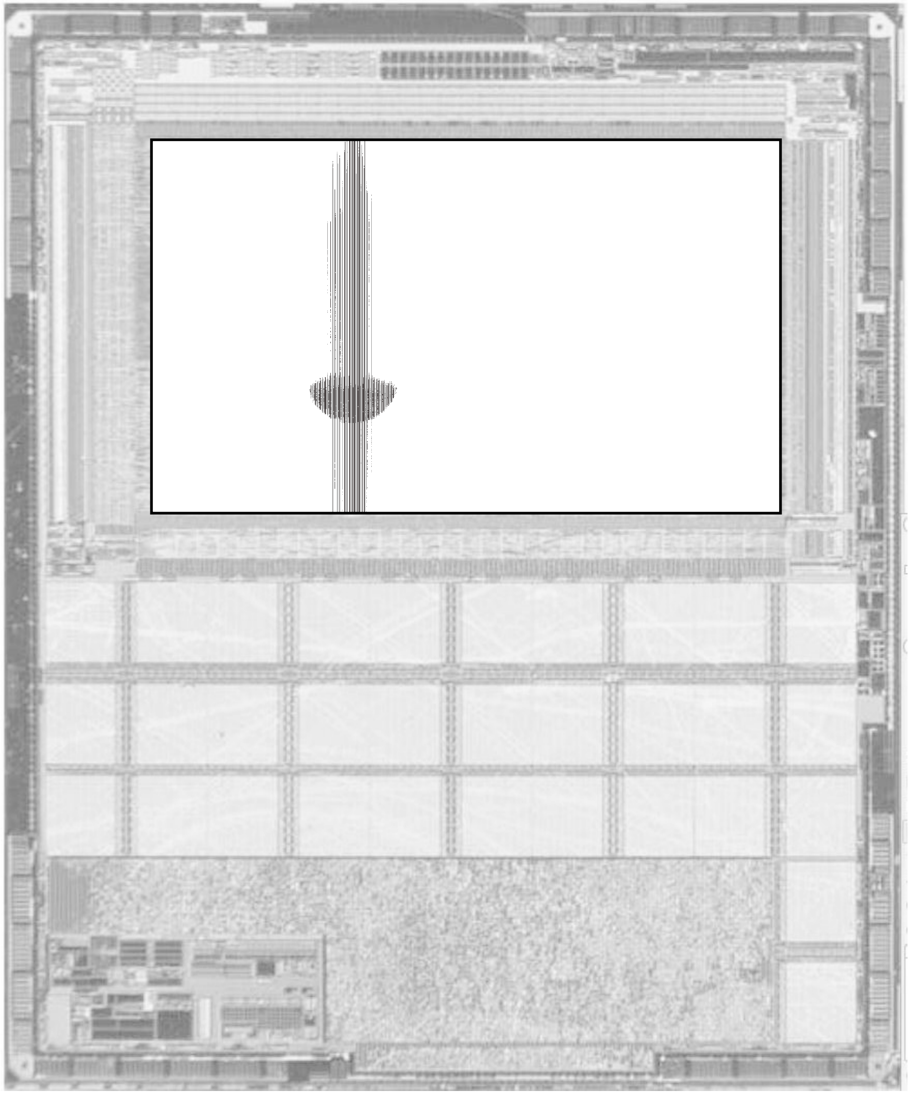
Read Flash during exposure

First faults obtained after 210 seconds of exposure

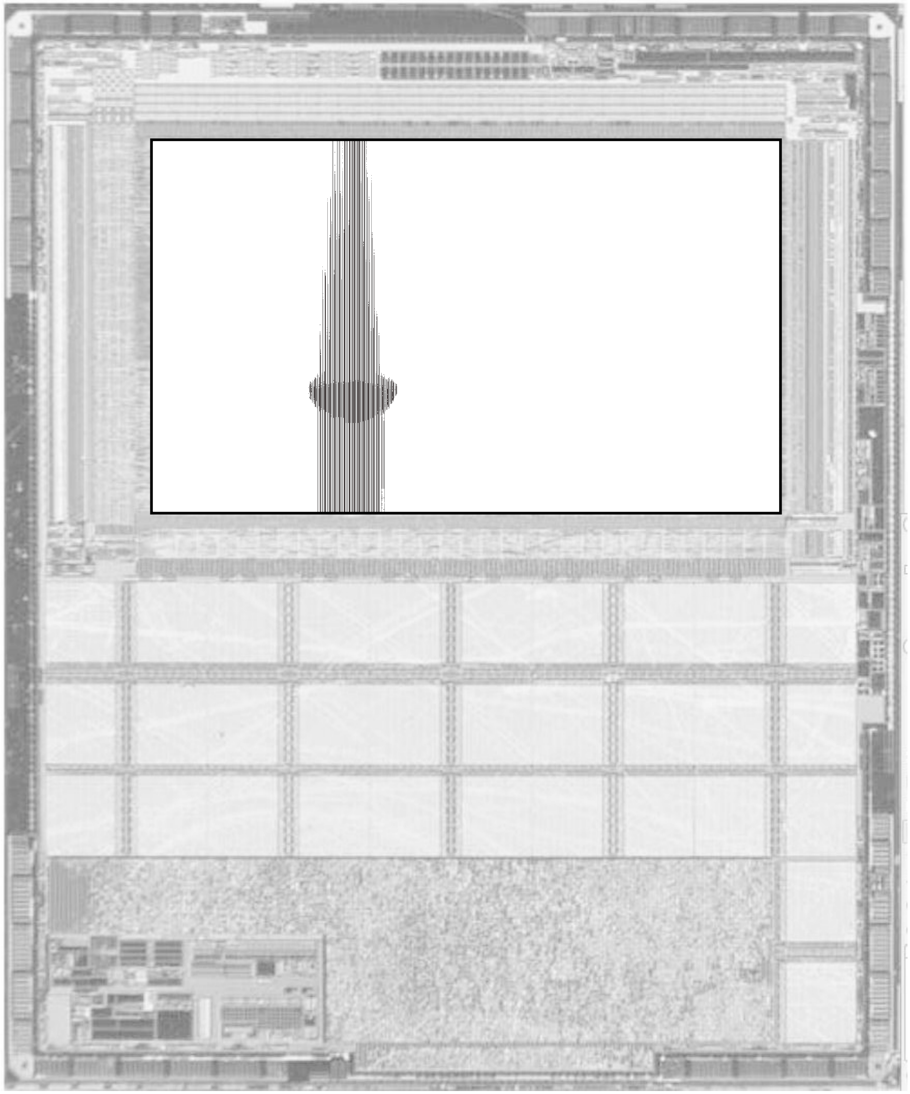


red: “1” to “0” corruption

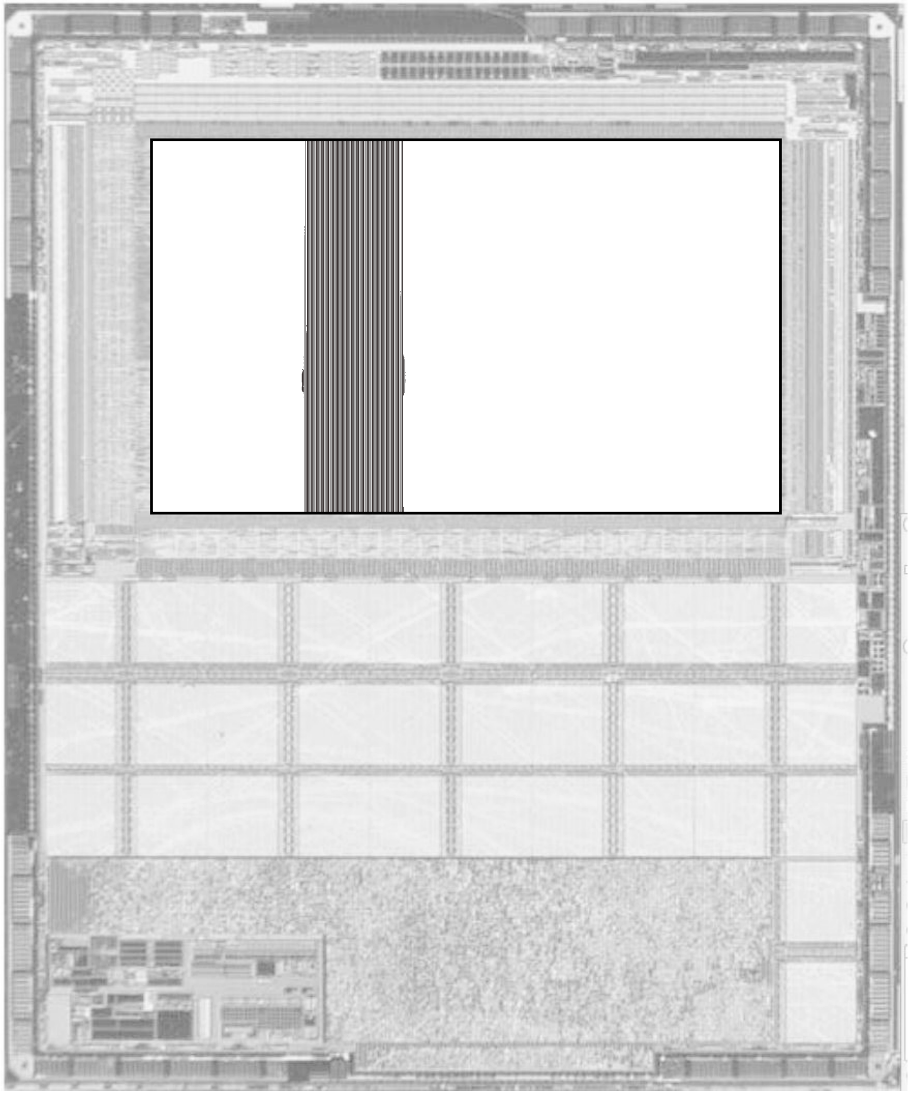
40 seconds later…



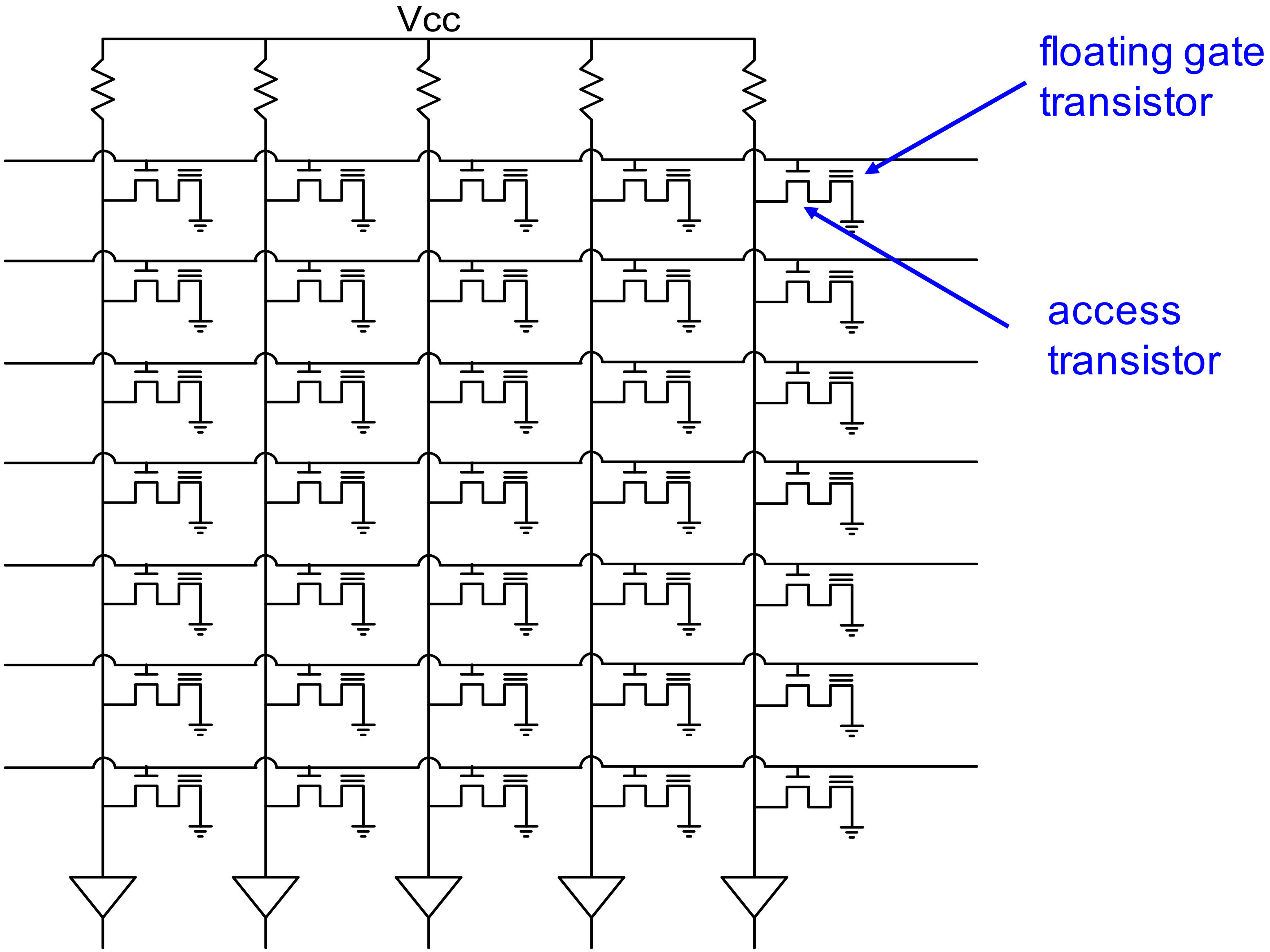
then 40 more…



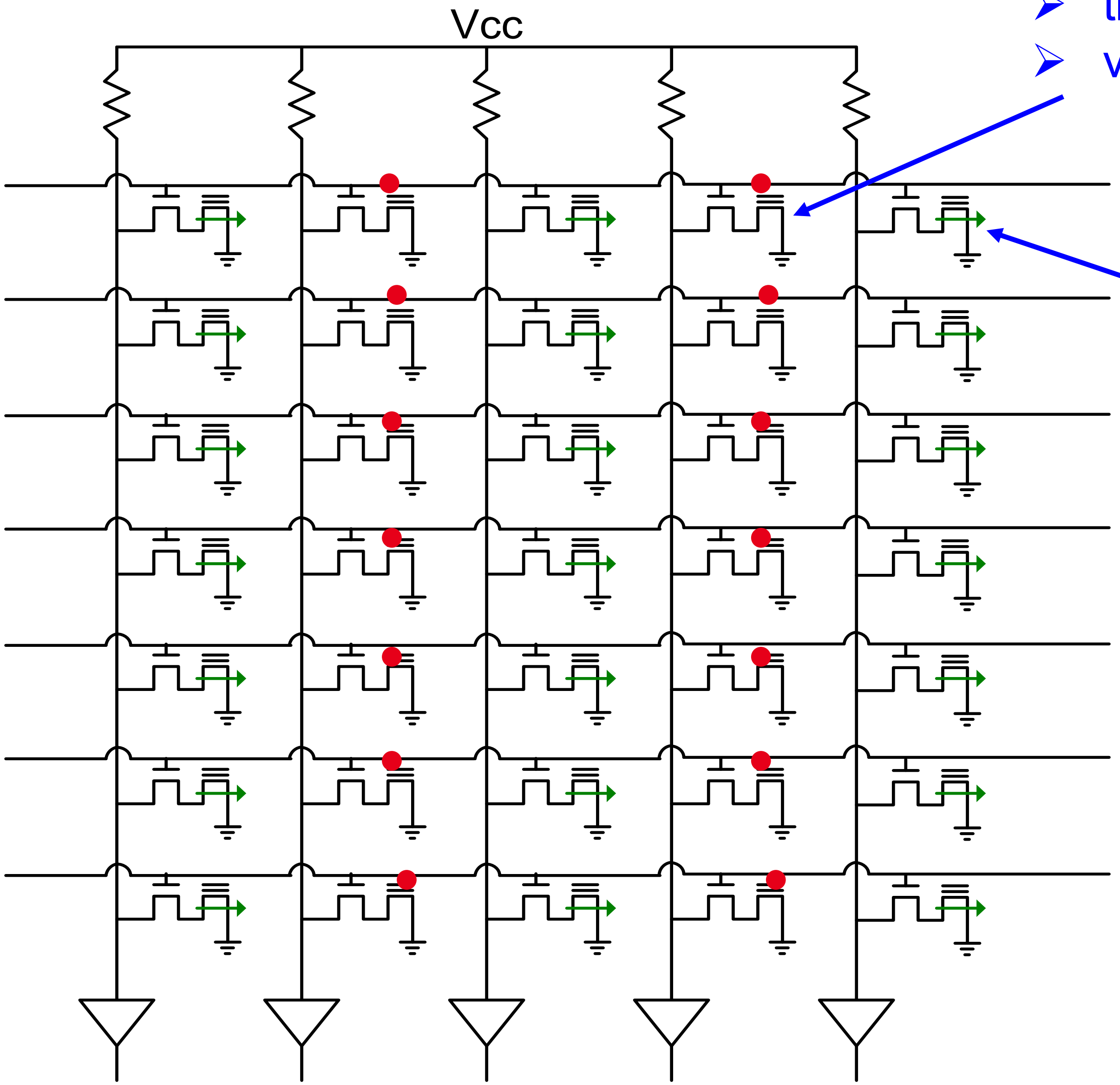
and finally



What happened?



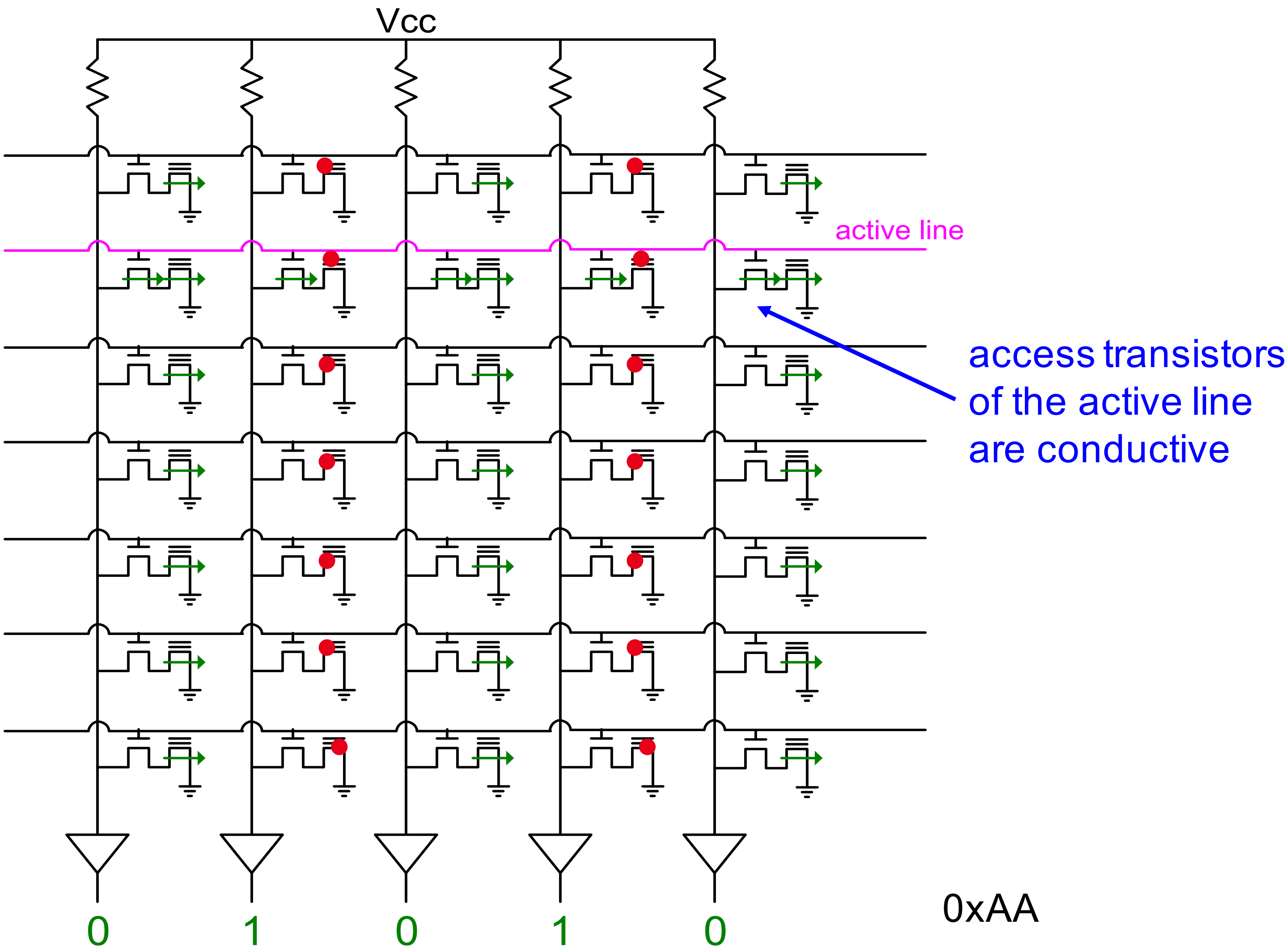
Data is stored in the floating gates



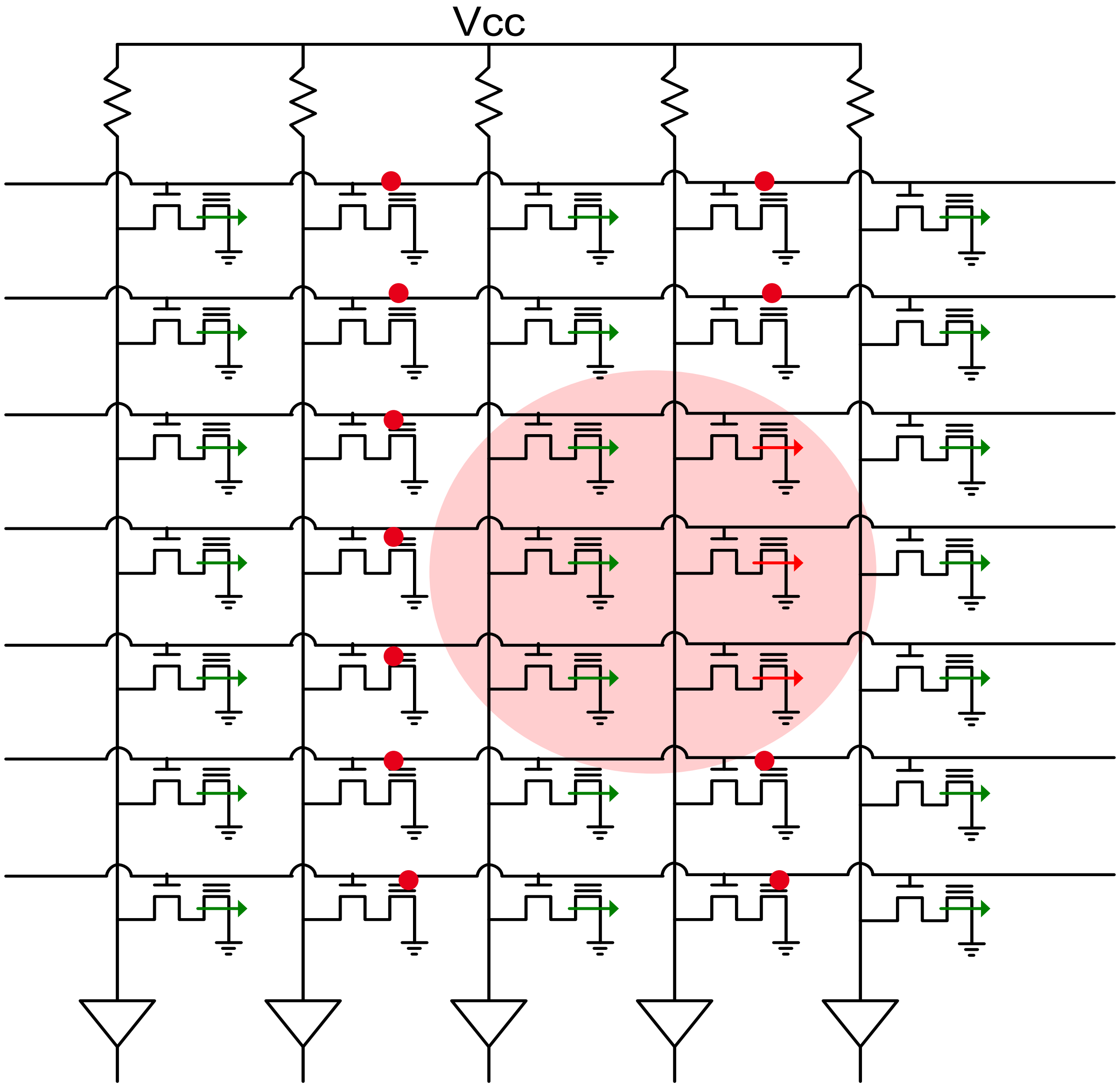
- charge in the floating gate:
  - transistor is blocked
  - value 1 is stored

no charge in the floating gate:
- transistor is conductive
- value 0 is stored

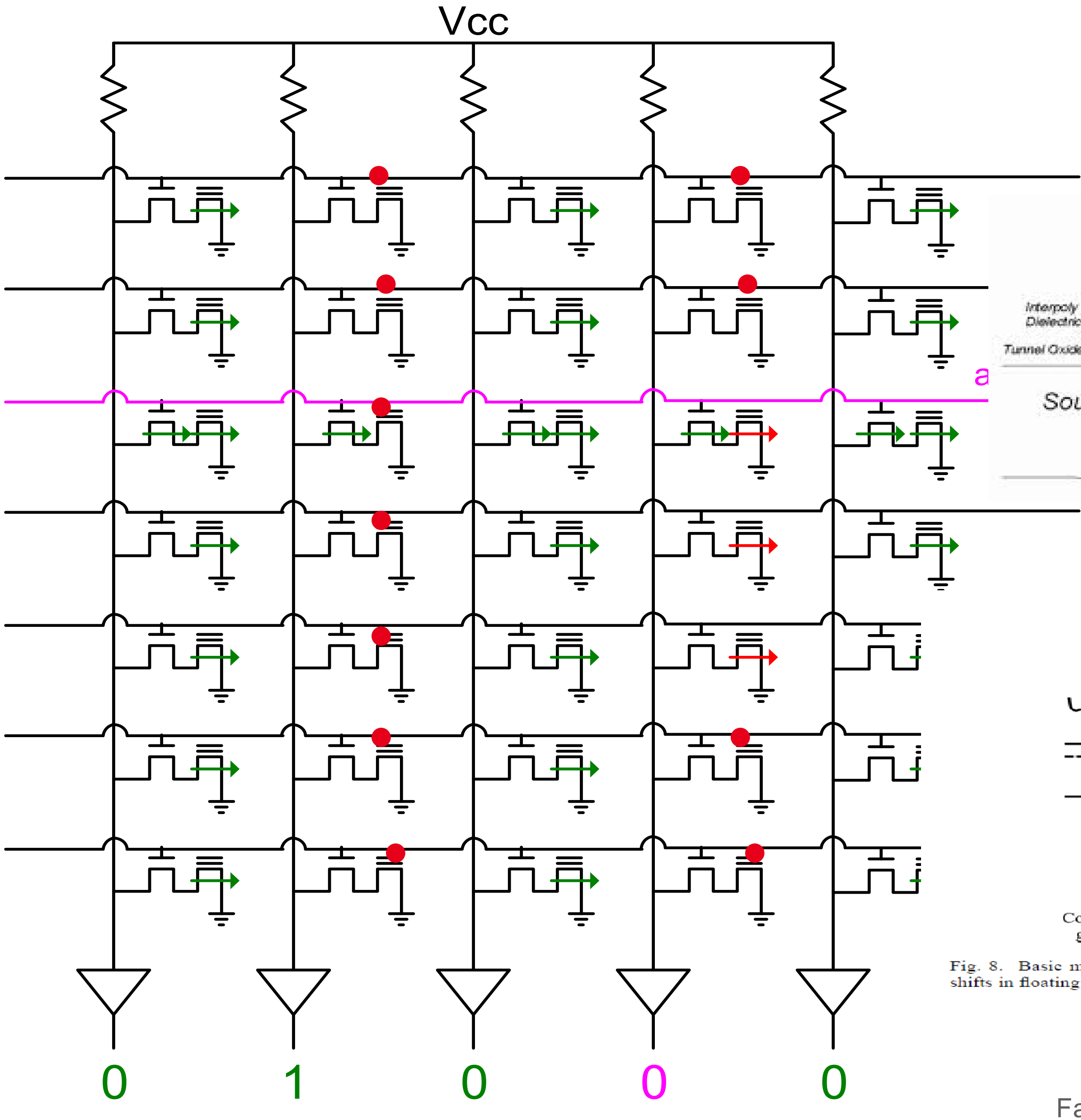
Access to the floating gates

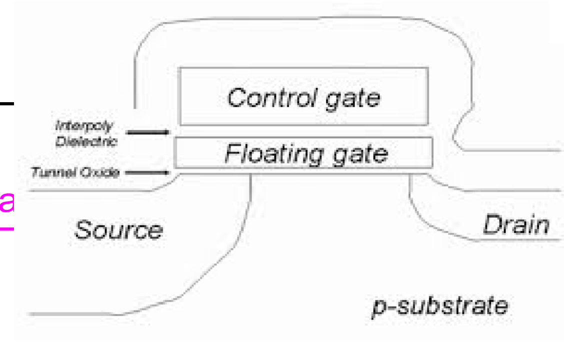


X-ray exposure : we discharge the floating gates



Access to the data





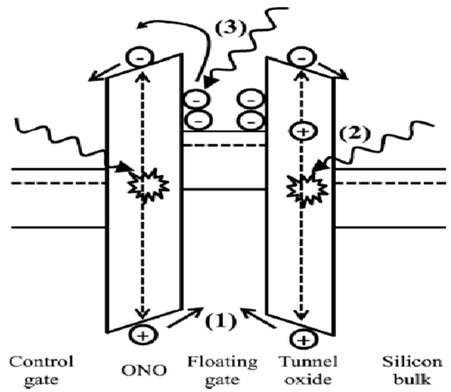
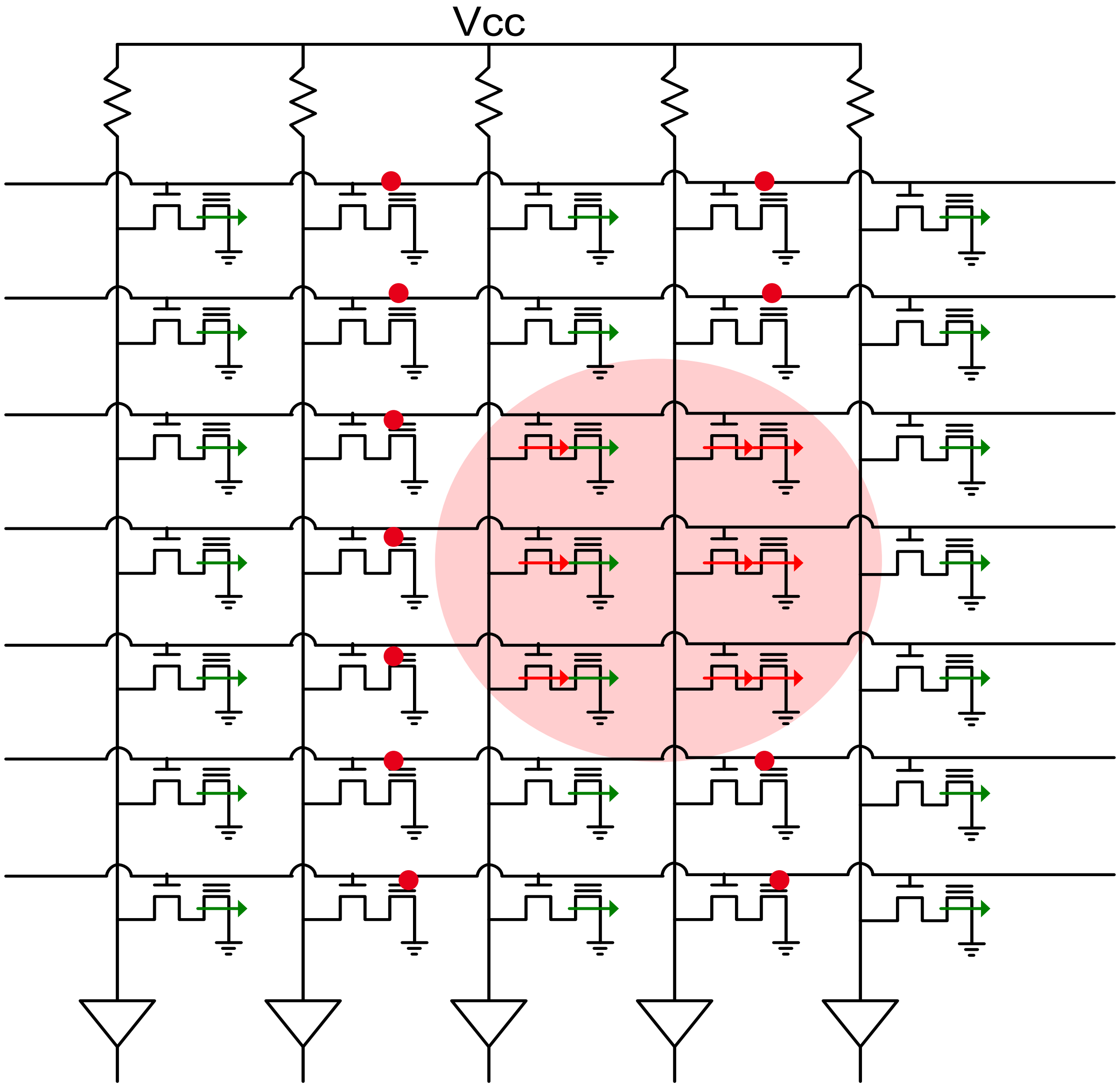
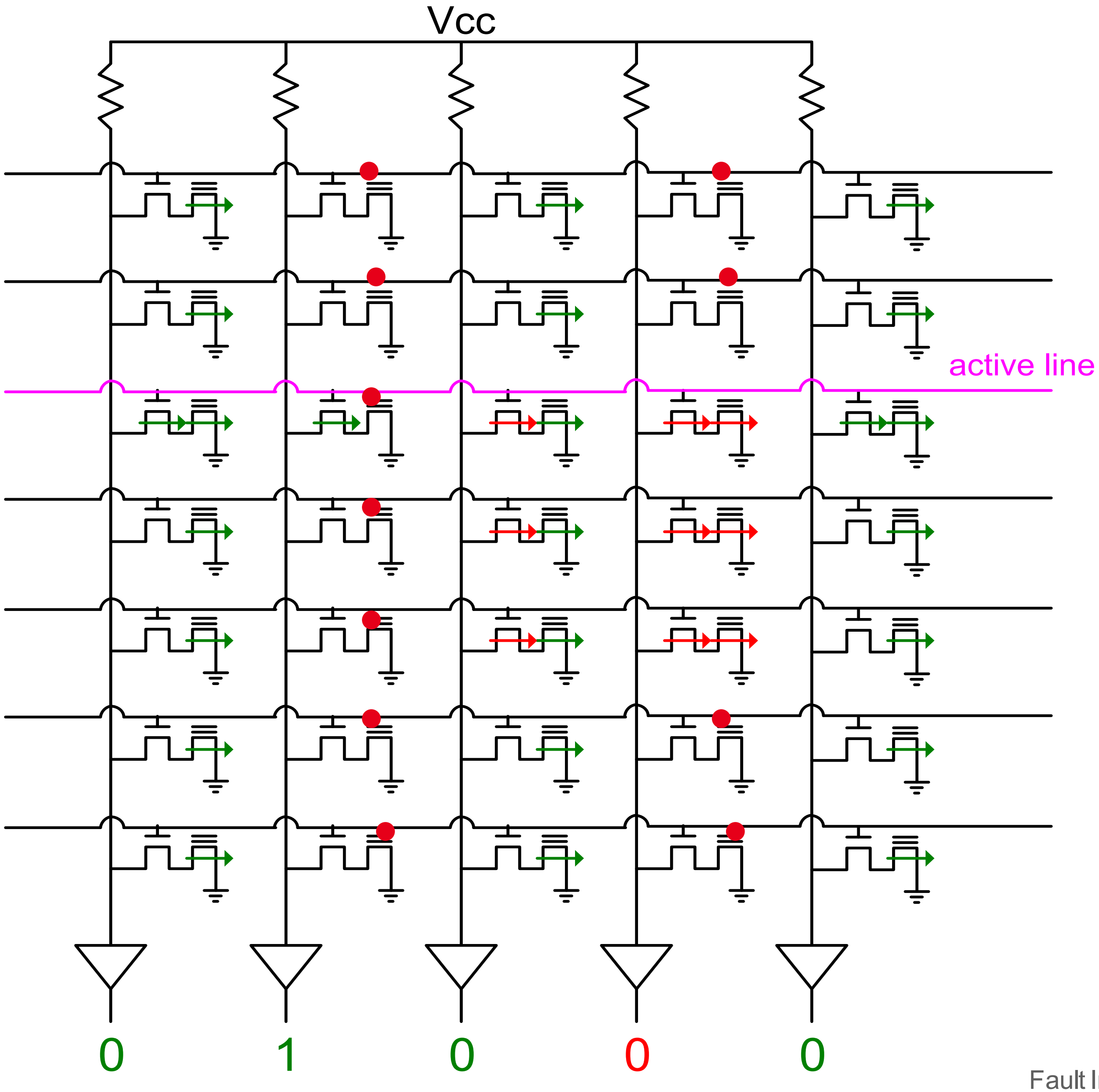


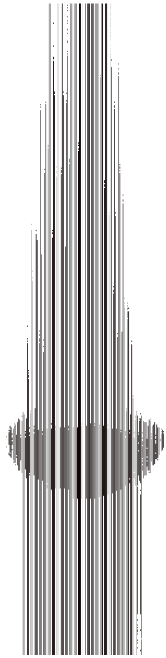
Fig. 8. Basic mechanisms for total ionizing dose induced threshold vo shifts in floating gate cells. After [23].

X-ray exposure continued : we semi-permanently switch on access transistors

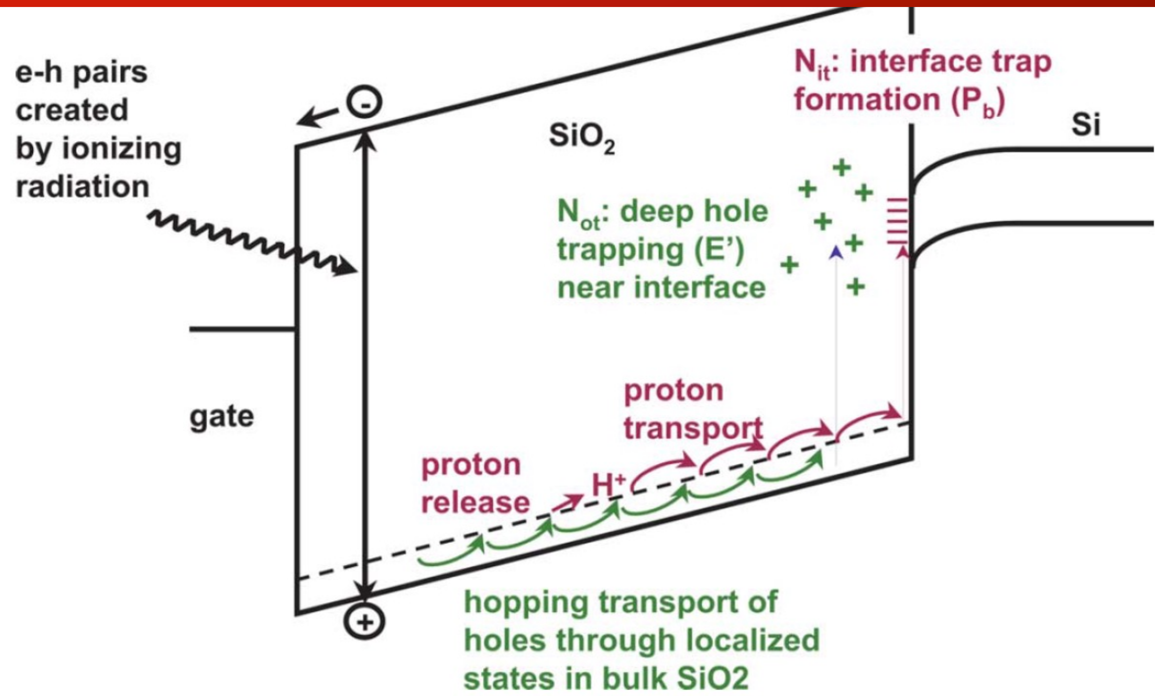


Column errors



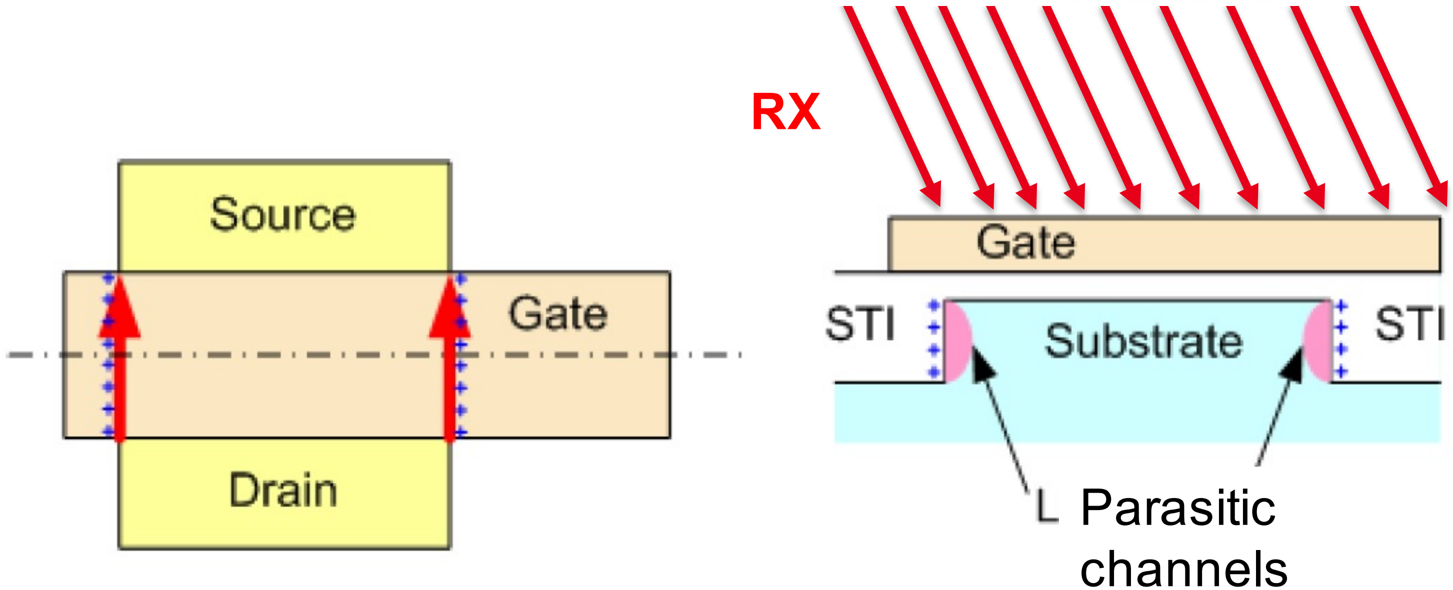


CHARGED TRAPPED IN THE OXIDES (GATE OX / SHALLOW TRENCH ISOLATORS)



Carriers trapped in gate oxide:

Carriers in STI:



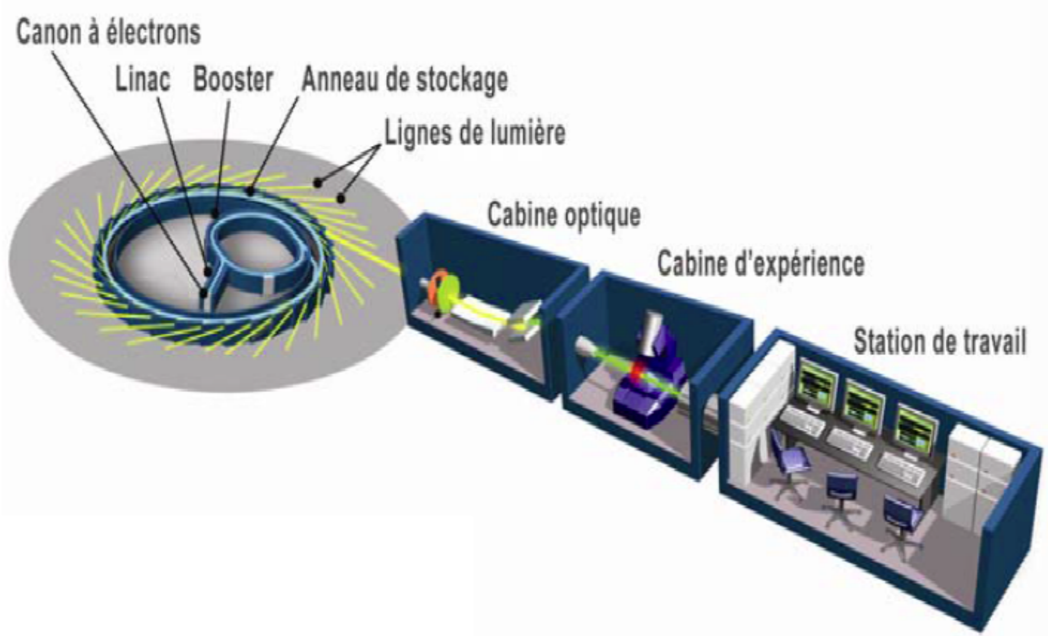
NMOS transistor

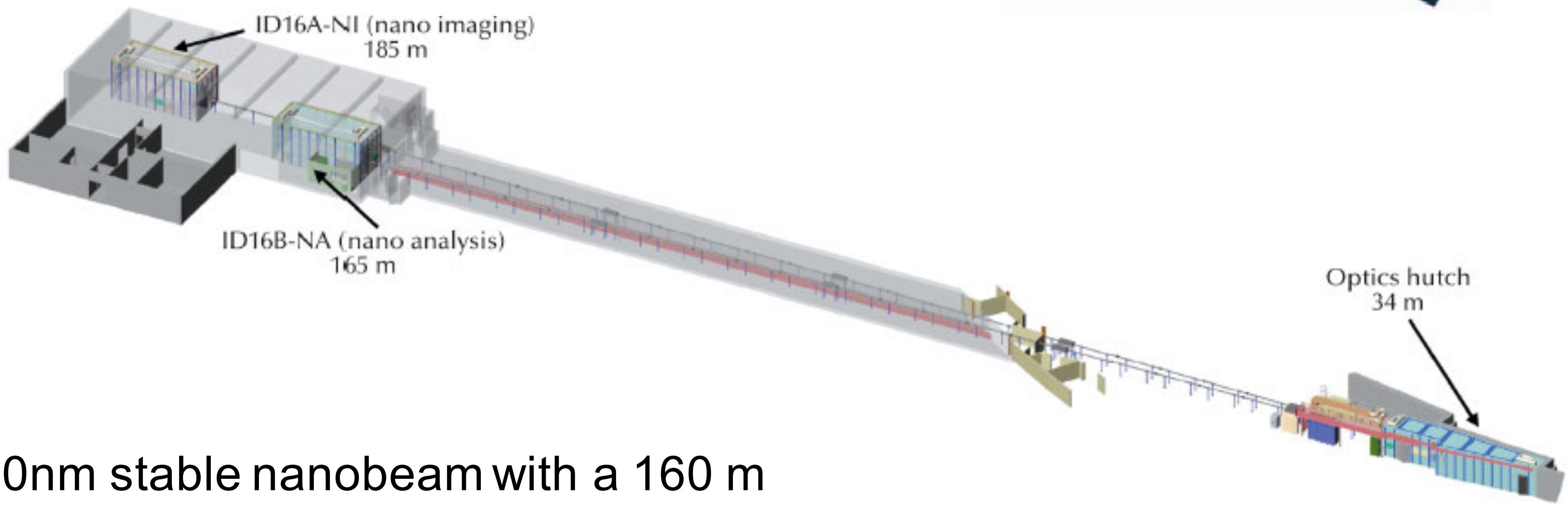
NANOFOCUS → ESRF GRENOBLE

500 m

SYNCHROTRON SETUP

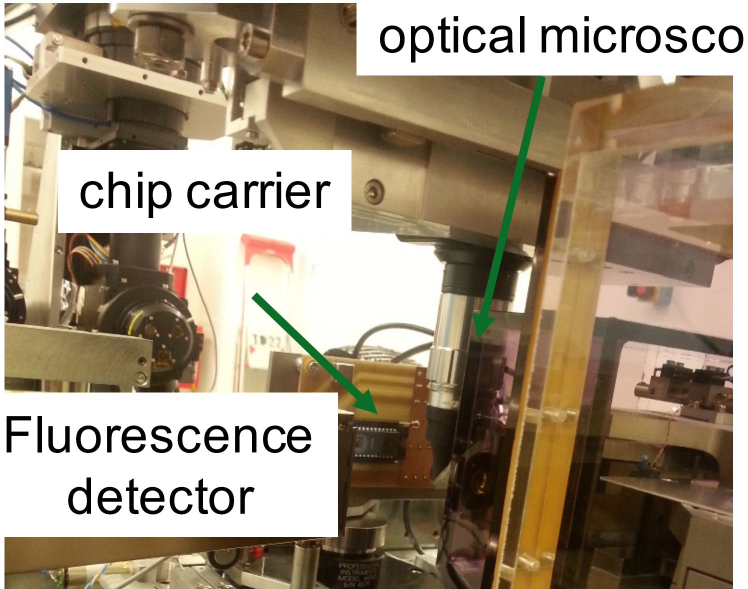
- Electron packets circulate in the loop
- Photon emitted w/h bending magnets and undulators

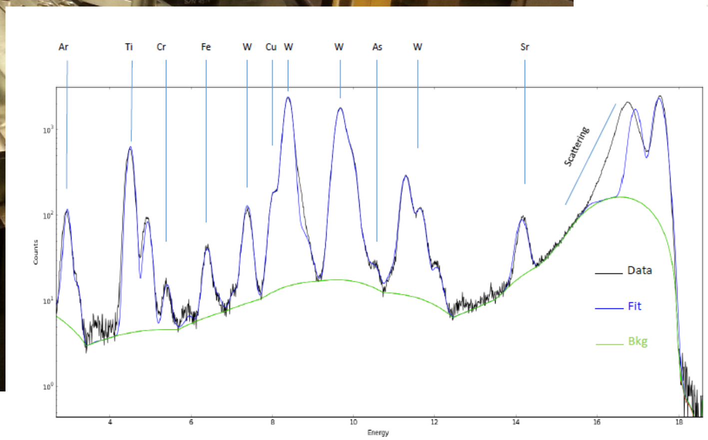


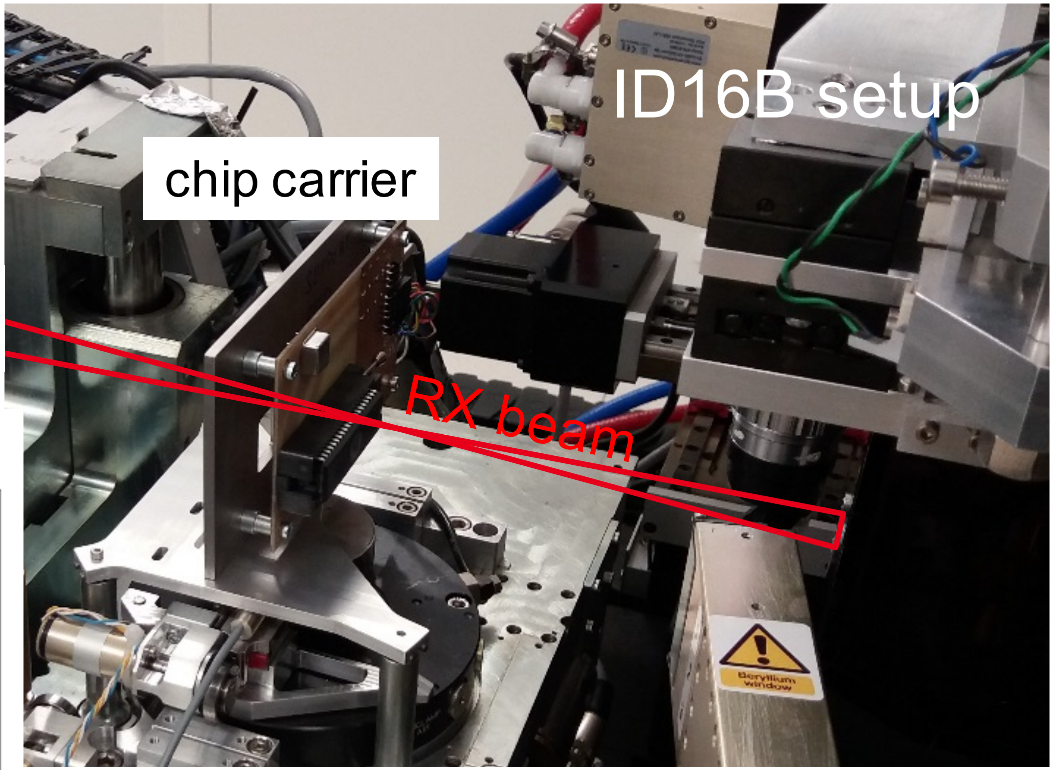


60nm stable nanobeam with a 160 m focalization length

- **Motivation: feasibility study of an x-ray attack for smart cards security => Single transistor !**







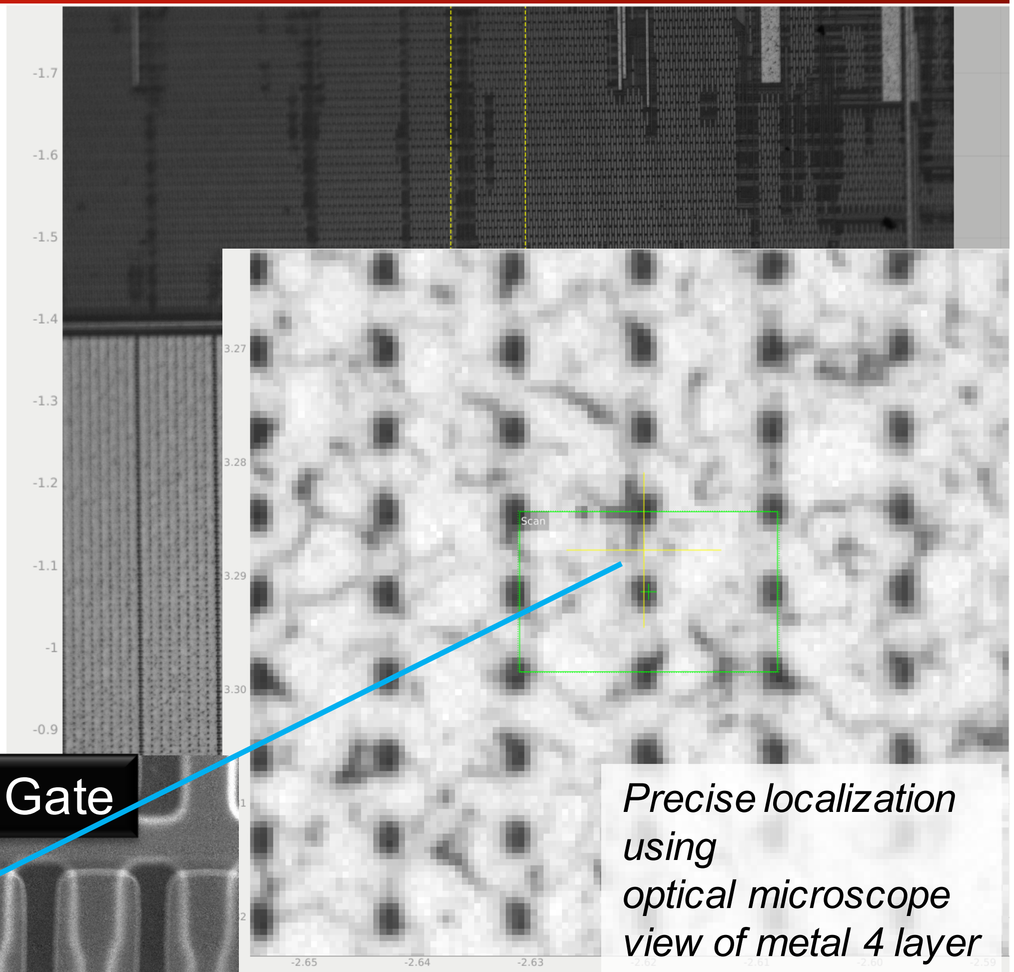
ATTACKS EXPERIMENTS RESULTS ON FLASH

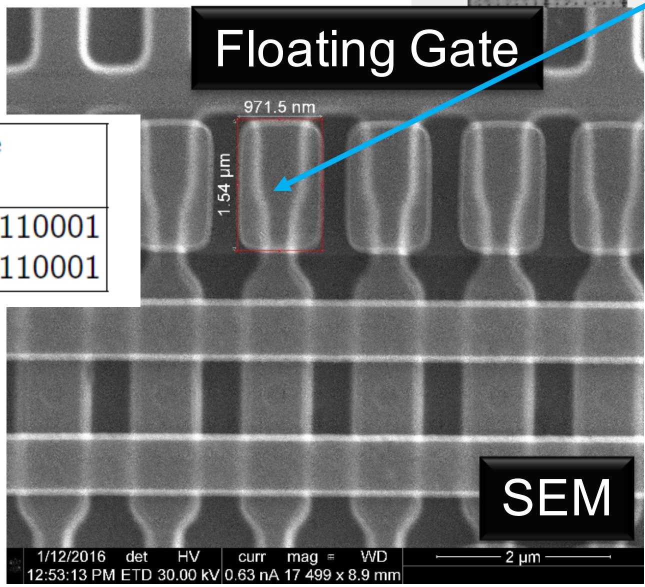
Localization of each **Flash** memory cells using the Optical microscope view of metal 4 layer (non destructive)

Electrons removed from floating gates : 1 -> 0 of single cells.

Demonstration of an attack on a Verify PIN program loaded in flash
- Localization of Flash address to be modified
- Software modification

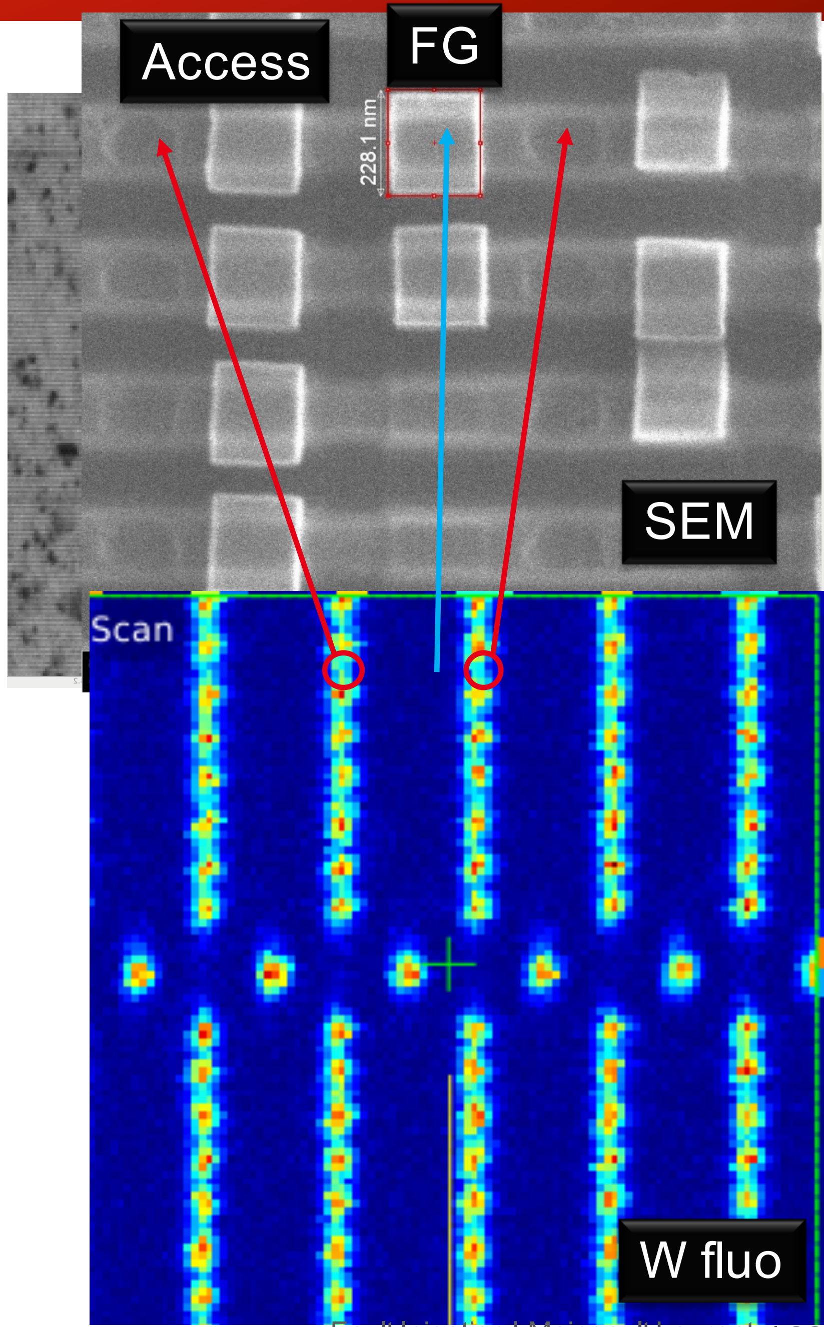
Instruction	hexadecimal code	binary code
BRNE .-84	0xf6b1	1111011010110001
BREQ .-84	0xf2b1	1111001010110001





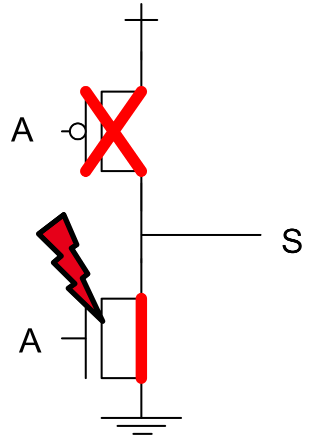
- **Experiment**
  - Needs fluorescence imaging => W contact (~ 50 nm resolution image)
  - Local x-ray attack of a single **Flash Nor** memory cell before or after a simple reading of the memory block
  - Down to 90 nm

Erase of the memory cell
1 -> 0

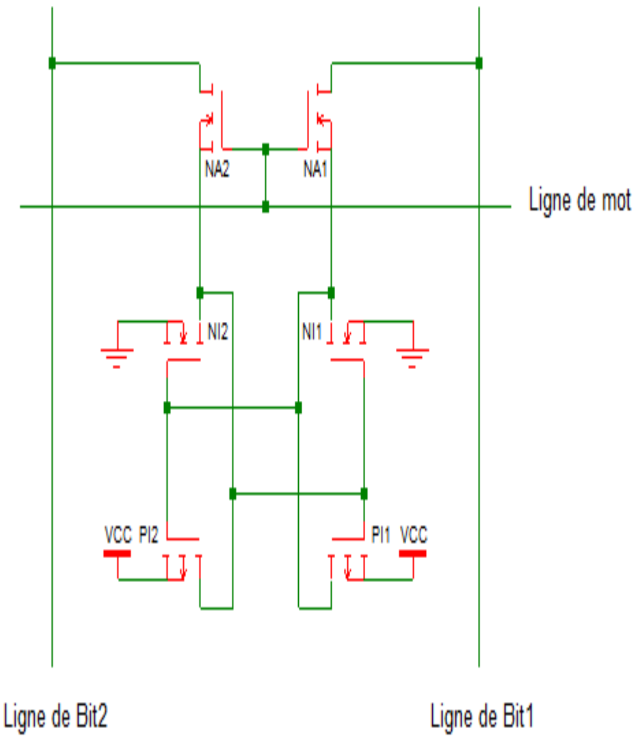


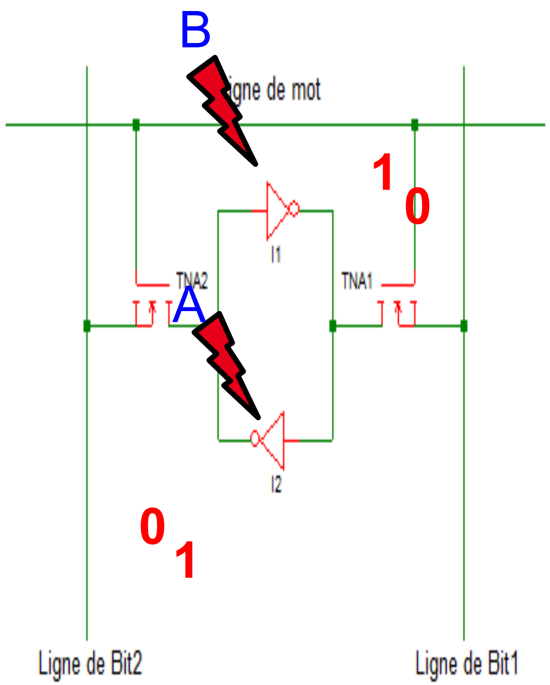
N MOS TRANSISTOR => CONDUCTOR WITH X EXPOSURE

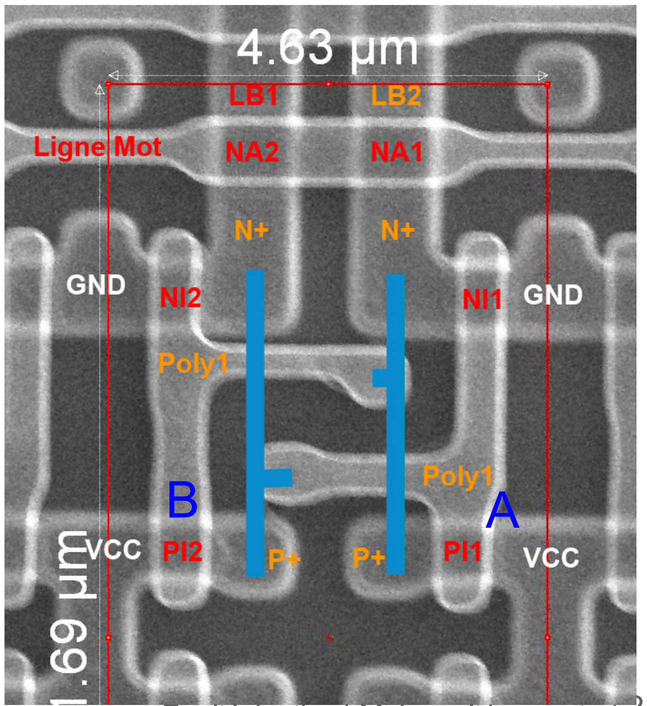
=> EASY TO STUCK AN INVERTER TO 0 AT THE OUTPUT



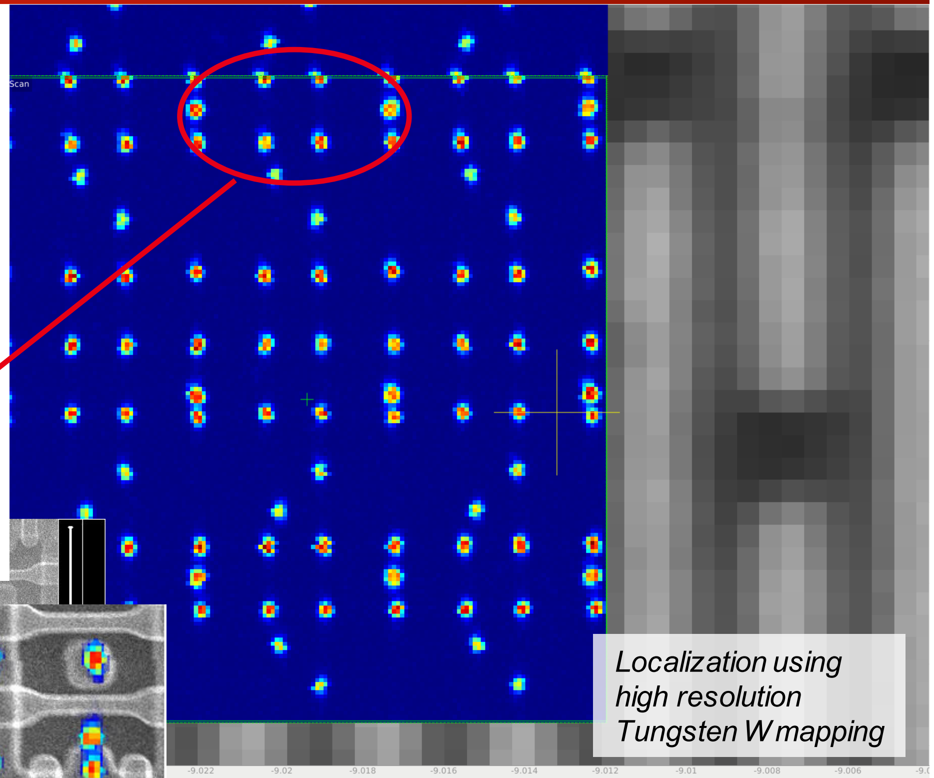
- **Picture : Active areas N ≡and P and Polysilicon lines**
- **Metal M1 (blue)**

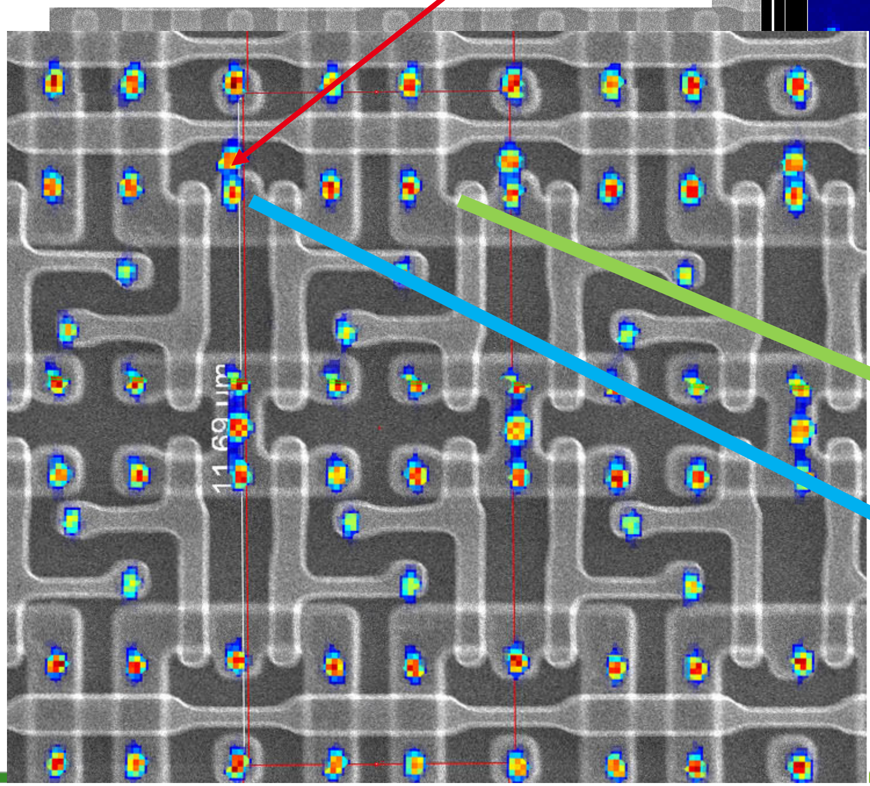






- **Experiment**
  - Local x-ray attack of a single **RAM** memory cell
  - The precise address of the single bit can be retrieved
  - Each memory cell can be set or reset
  - Down to **55 nm**





MOS-N=> Permanent conductor

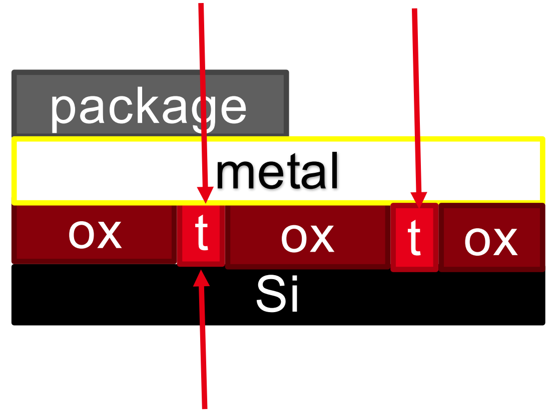
Set = output stick to 1

Reset = output stick to 0

X-RAYS, AN ENHANCED LASER FAULT INJECTOR ?

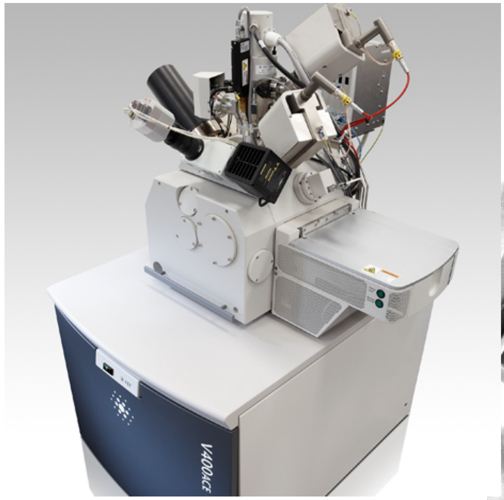
X (~ 10 keV)

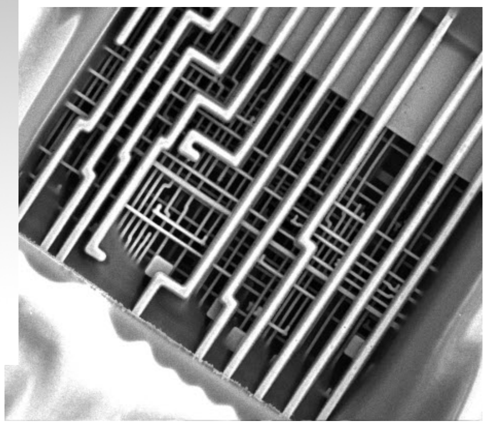
- Wavelenght < 1 nm (address a single memory cell down to 55 nm node)
- Package, thin metal layers → ~ transparent
- Attack NVM memories



- **Physical effect is different**:
  - Impossible to synchronize below 1 ms
  - No transient faults possible (no X Beam Induced Current observed)
  - Semi-permanent effect on transistor (needs an annealing to restore its normal state)

Nano-beam X ray <=> Non invasive FIB acting on transistors





PERSPECTIVE FOR X RAYS ATTACKS

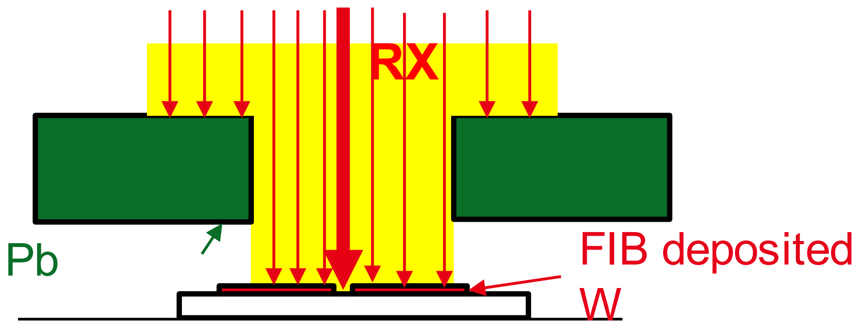
- Synchrotron: expensive (2x FIB V400) / availability

- Other X-ray generators : spot size still large. May change ?

2 paths for further developments

1. Lower attack rating

- Faster annealing ?
- Use a generic X generator w/h improved masking techniques



2. Advanced attacks w/h synchrotron radiation

- Limit on the technology node ?
- Attacks on glue logic

FIN

C. Tarnovsky : Deconstructing a ‘Secure’ Processor. In: Black Hat Federal 2010 (2010).

Rino Micheloni, Luca Crippa, Alessia Marelli, "Inside NAND Flash Memories", pp. 537-571

T.R. Oldham, Fellow, IEEE, and F.B. McLean, Fellow, IEEE, "Total Ionizing Dose Effects in MOS Oxides and Devices", *IEEE Trans. Nucl. Sci.*, vol. 50, pp. 483-499, June 2003.

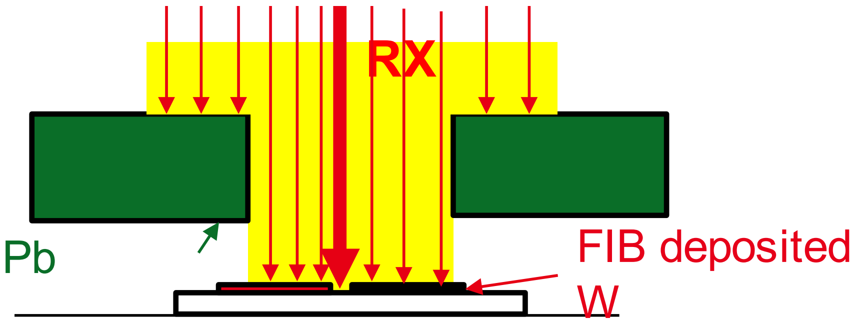
E. Snyder, P. McWhorter, T. Dellin, and J. Sweetman, “Radiation response of floating gate EEPROM memory cells,” *IEEE Trans. Nucl. Sci.*, vol. 36, pp. 2131–2139, Dec. 1989.

G. Cellere, A. Paccagnella, A. Visconti, M. Bonanomi, S. Beltrami, J. Schwank, M. Shaneyfelt, and P. Paillet, “Total ionizing dose effects in NOR and NAND flash memories”, *IEEE Trans. Nucl. Sci.*, vol. 54, pp. 1066–1070, Aug. 2007.

S. Gerardin, M. Bagatin, A. Paccagnella, K. Grürmann, F. Gliem, T. R. Oldham, F. Irom, and D. N. Nguyen, "Radiation Effects in Flash Memories", *IEEE Trans. Nucl. Sci.*, vol. 60, no. 3, pp. 1953–1969, June 2013
S. Anceau, P. Bleuet, J. Clédière, L. Maingault, J.L. Rainard, R. Tucoulou : “Nanofocused X-Ray Beam To Reprogram Secure Circuits”, CHESS 2017, Taiwan.

Modifications de circuits électroniques avec l'utilisation de rayons X et FIB

- Laser annealing ?
- Use a generic X generator w/h improved masking techniques



Advanced attacks w/h synchrotron radiation

- Lowest technology node ?
- Attacks on glue logic

Contacts:
Stephanie.anceau@cea.fr
Jessy.clediere@cea.fr
Laurent.maingault@cea.fr