FPGA Assessment Methodology of Adverse X-Ray Effects on Secure Digital Circuits

Paolo MAISTRI
CNRS/TIMA Laboratory

BITFLIP 2025

The MITIX Project

- Modification non-Invasive de circuiTs Intégrés par rayons X (2021-2026)

ANR-20-CE39-0012

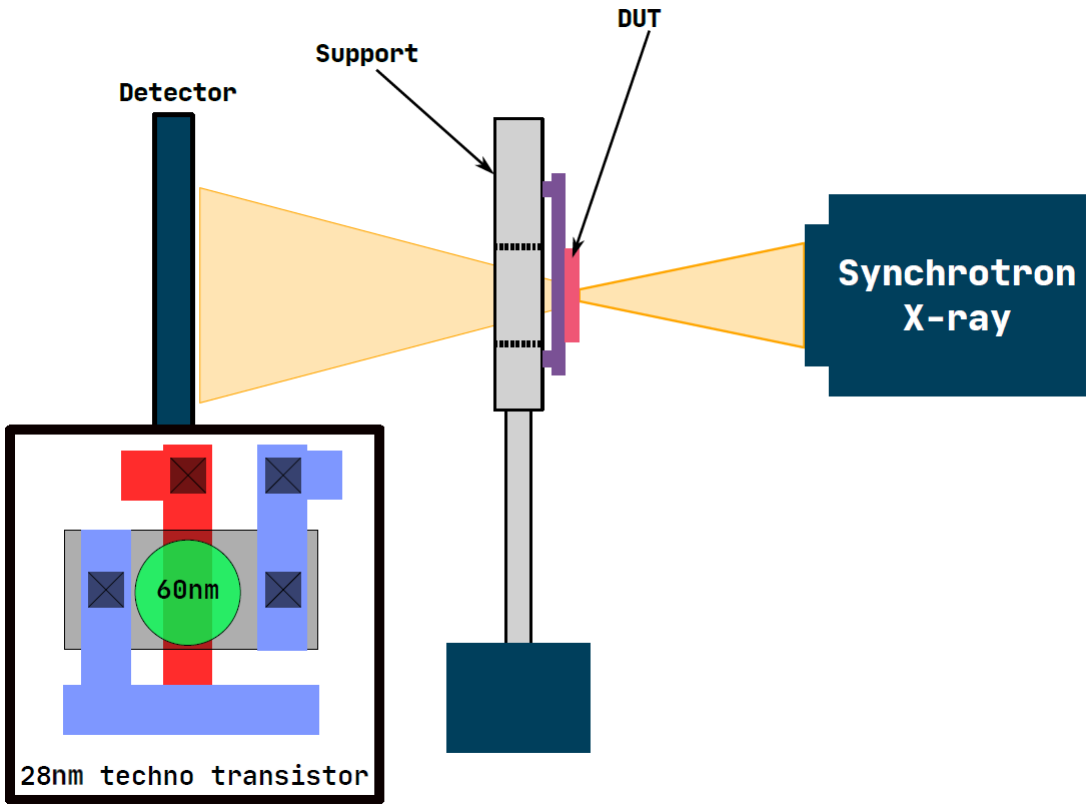
Thanks to:

Nasr-Eddine OULDEI TEBINA, PhD

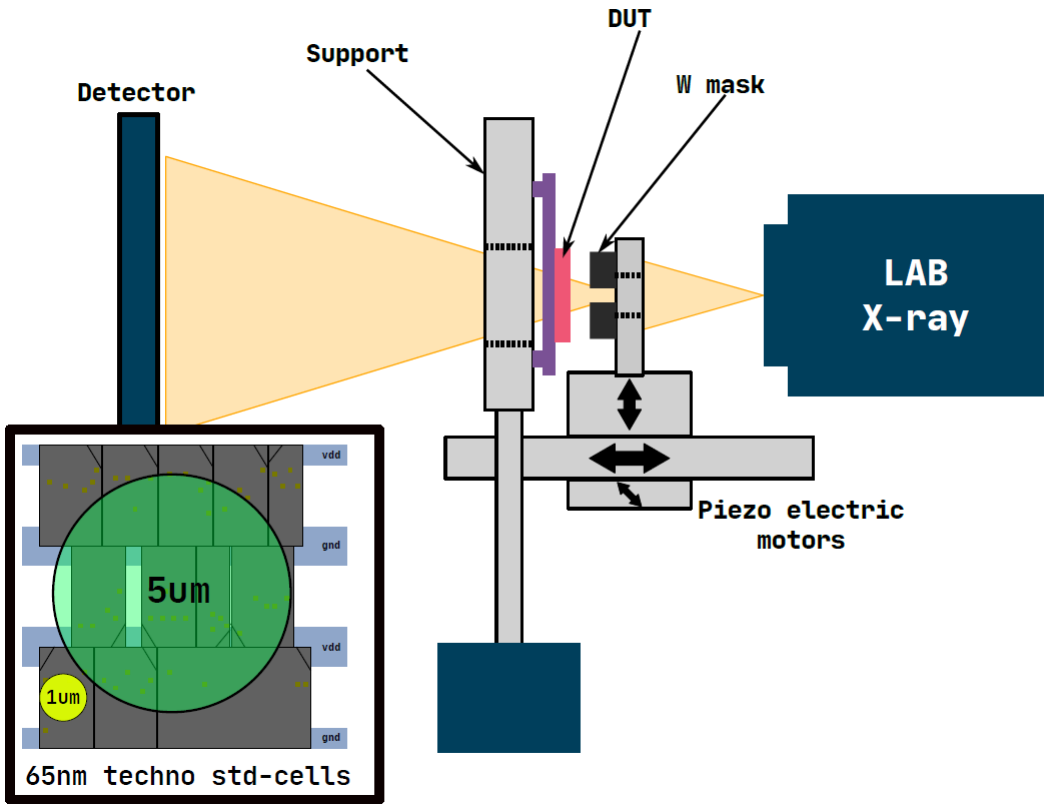
currently Head of Security Engineering @ Fortaegis Technologies (NL)

Synchrotron VS Lab Sources

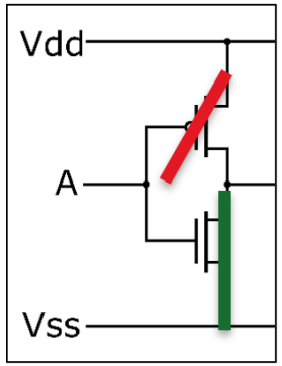
Synchrotron source



Laboratory source



X-Ray Fault Model



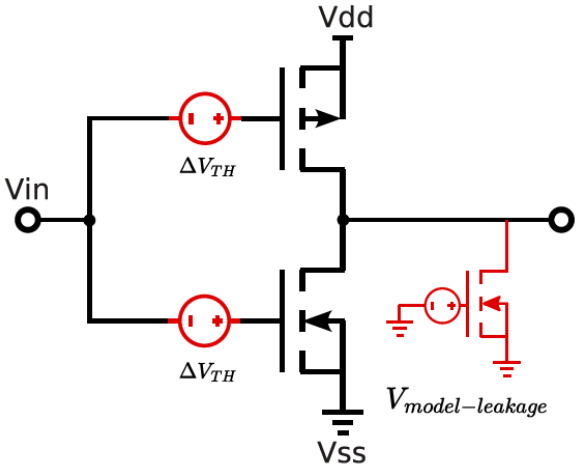
Pmos fully blocked

Nmos fully leak

- Faults are semi-permanent, can be removed with time and/or temperature
  - (Semi)-Persistent Fault Attacks
  - Circuit edit at the transistor level

(See previous Maingault's presentation for further details ☺)

- Main TID radiation effects on MOS structures:
  1. Threshold Voltage Shift (NMOS ▼, PMOS ▲)
  2. Leakage Current
     - Sub-Threshold (NMOS ▲, PMOS ▼), Static (NMOS ▲)
  3. Transconductance Degradation

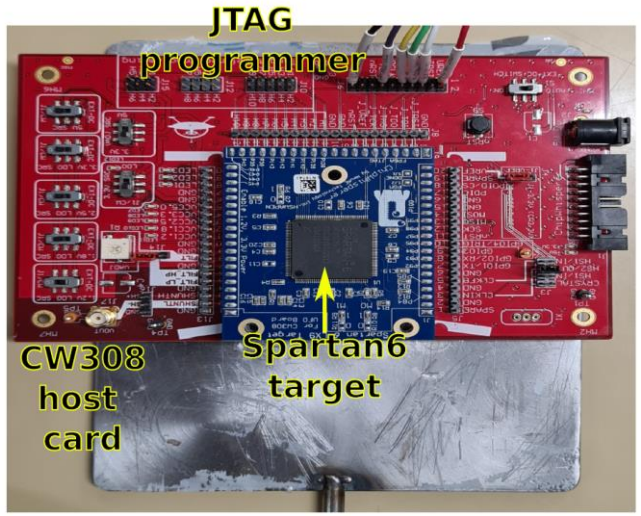


Motivation, Goal… & Outline

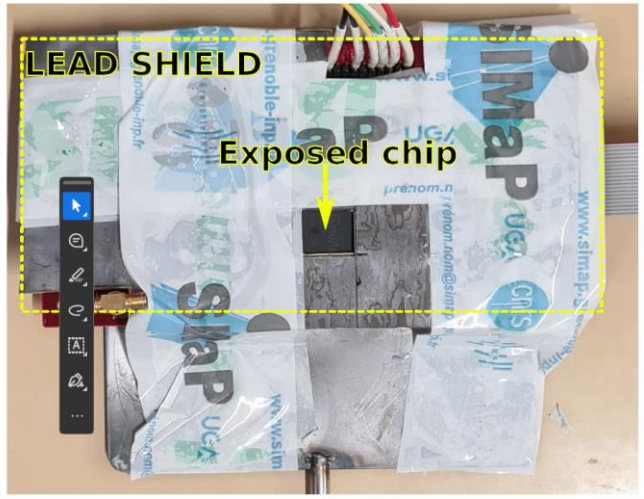
Is there an impact on security other than permanent faults?

- Impact of dose **before** fault occurrence [HOST24]
- Impact on **side channel** leakage [DATE24]
- Characterization of **FPGA** building blocks [TDMR25]

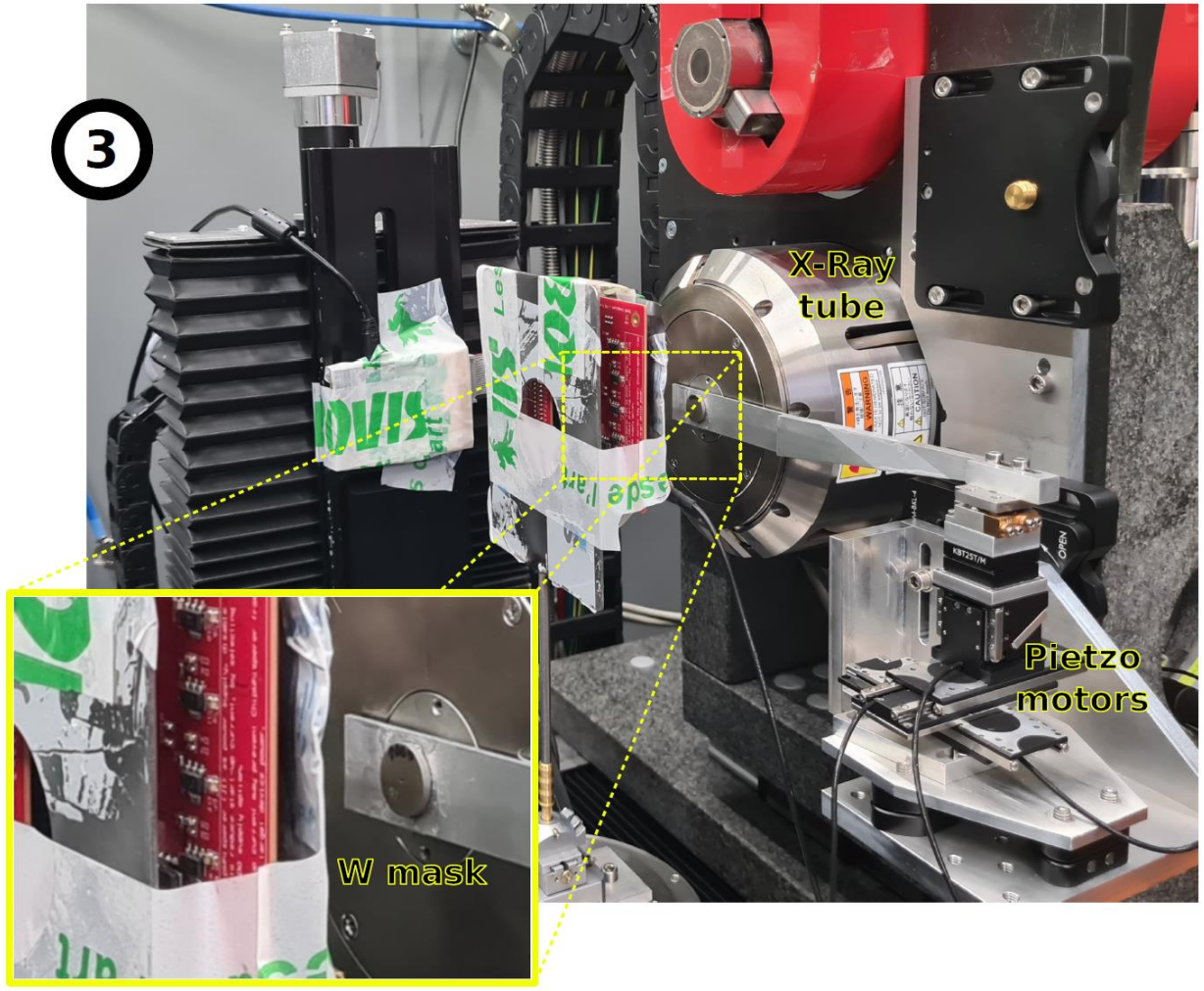
Lab Experimental Setup



1



2

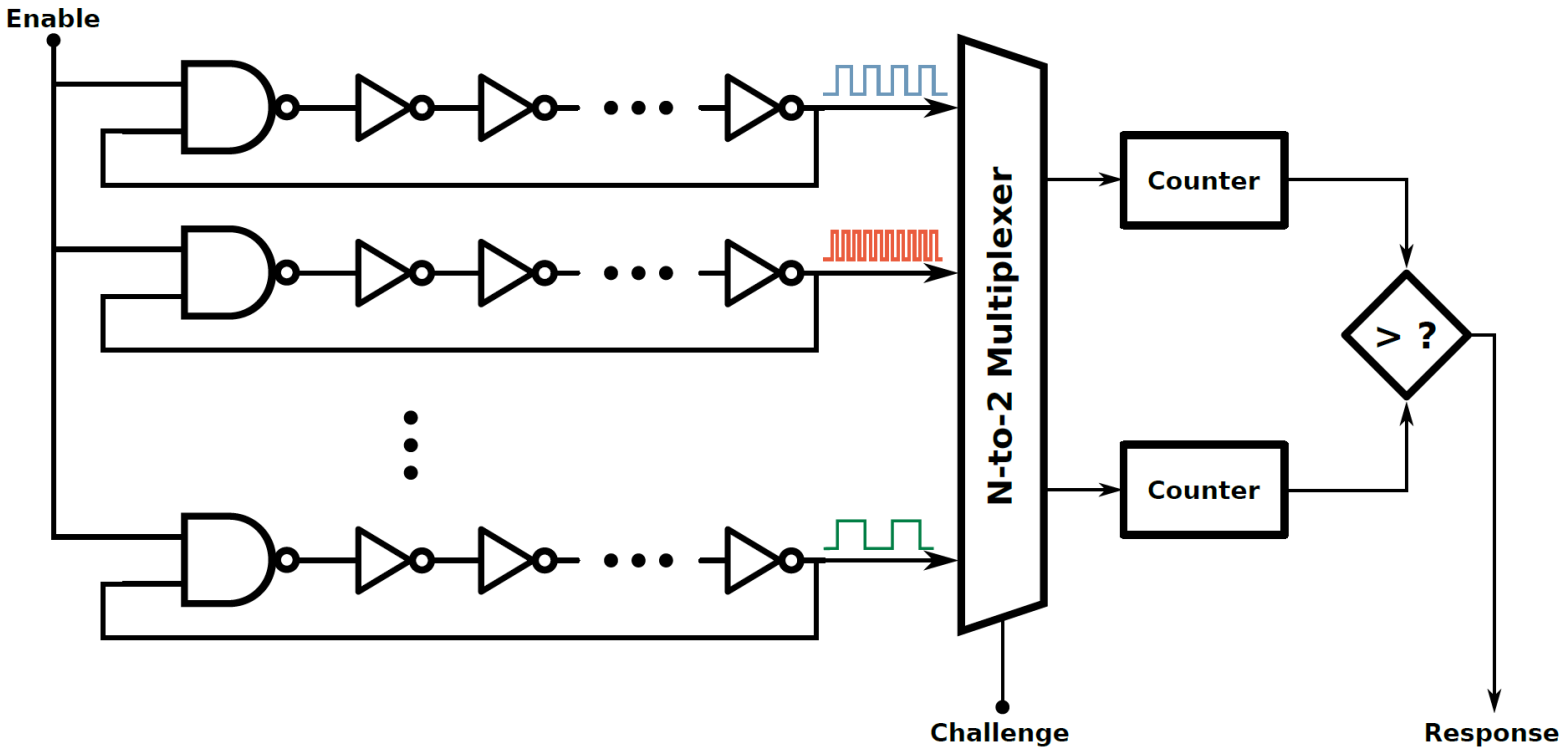


3

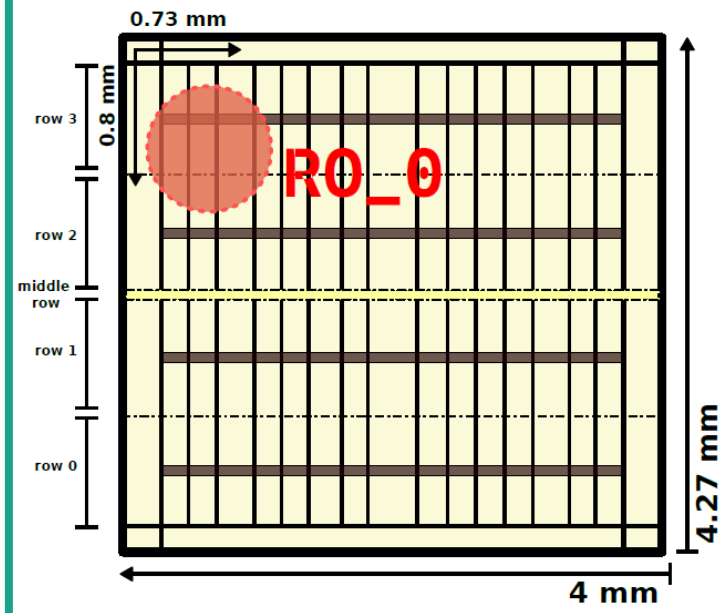
Primitive Biasing

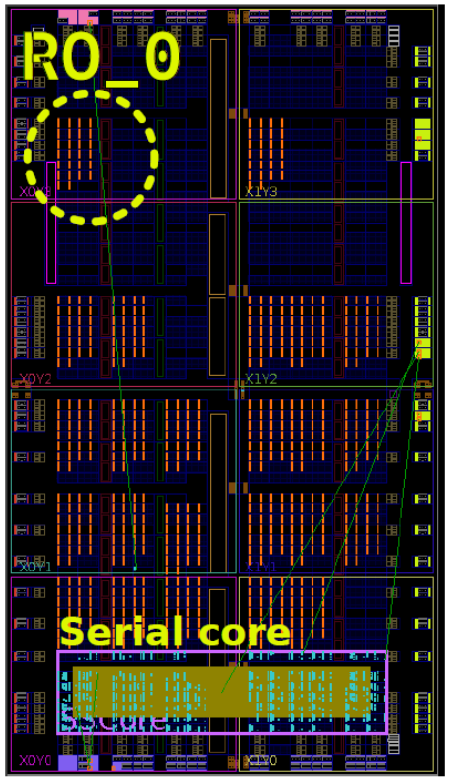
Ring Oscillator PUF

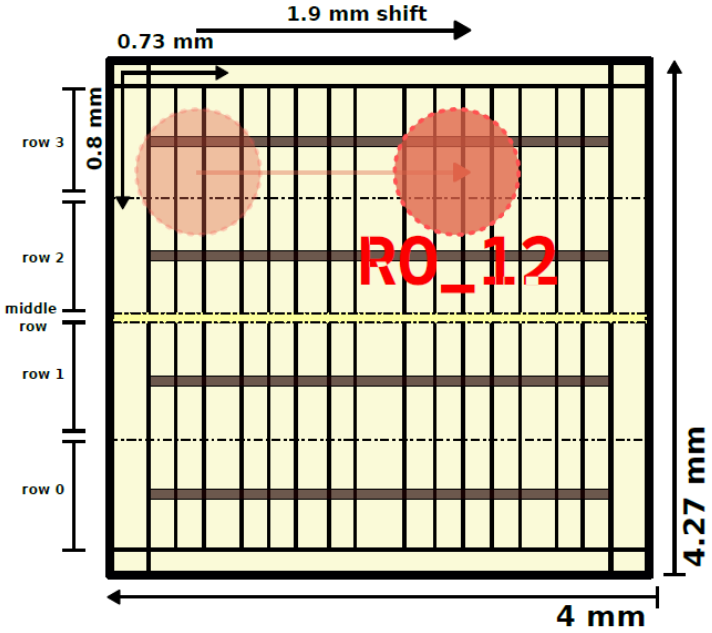
- Ring Oscillators, all same theoretical frequency
- Practically all different
  - Intra-die variations
  - Inter-die variations
- Each device unique
  - Identification
  - Key generation

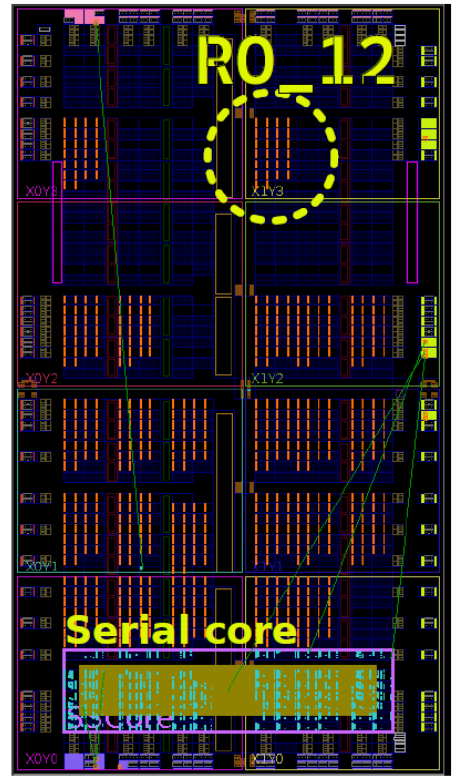


Target Architecture



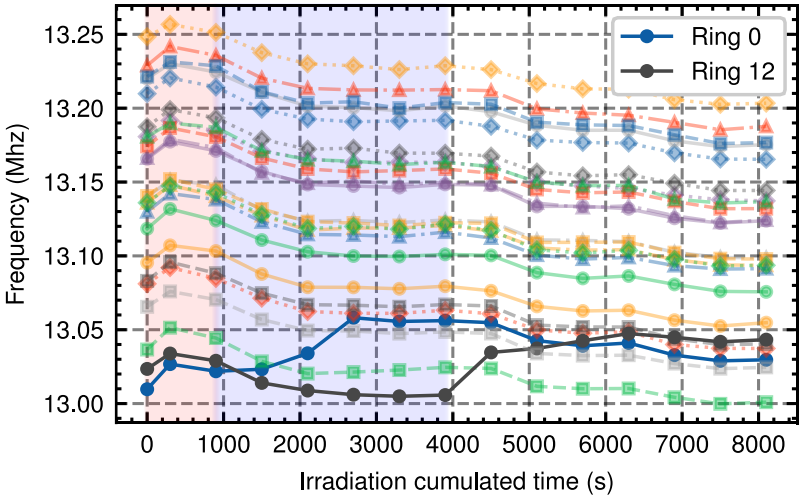






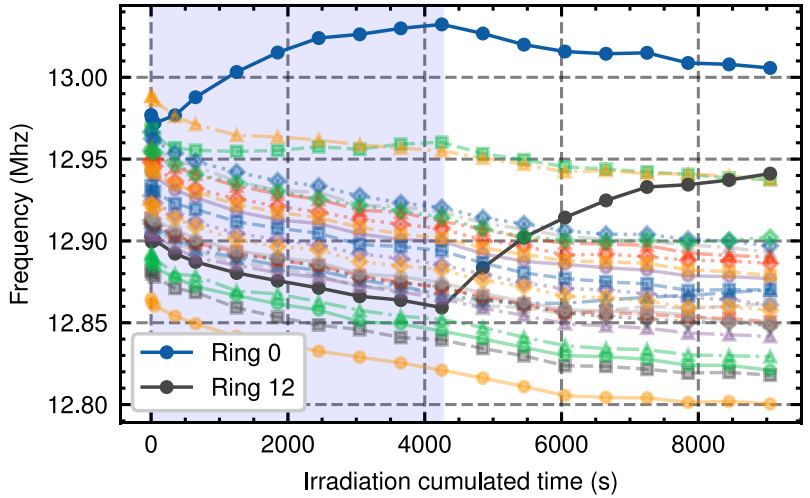
RO Frequency Biasing [HOST24]

POWER OFF



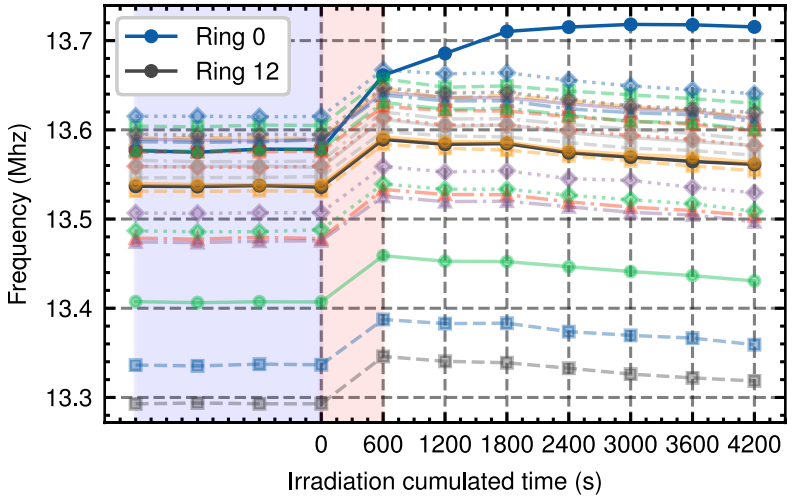
	RO_0	RO_{12}
$f_0(MHZ)$	13.01	13.01
$f_{max}(MHZ)$	13.06	13.054
Δf	+0.37%	+0.32%

POWER ON



	RO_0	RO_{12}
$f_0(MHZ)$	12.98	12.86
$f_{max}(MHZ)$	13.03	12.94
Δf	+0.43%	+0.64%

POWER ON (frozen)

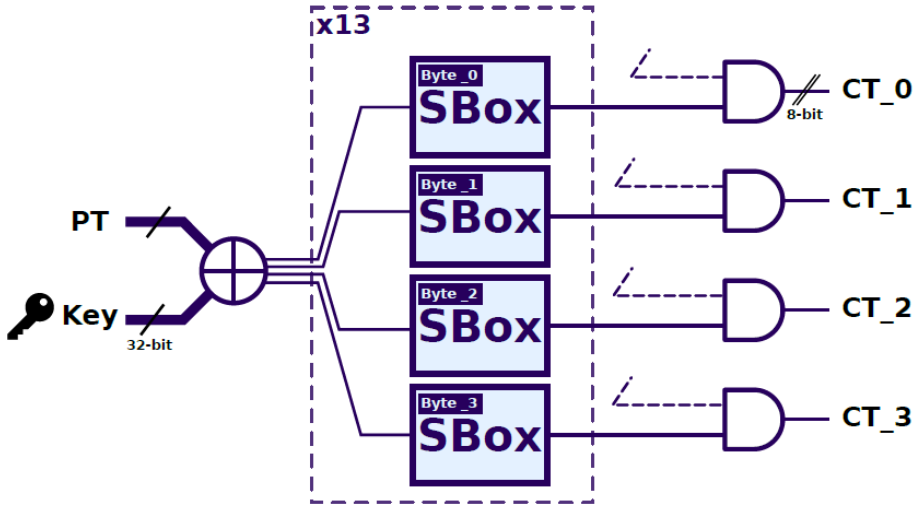


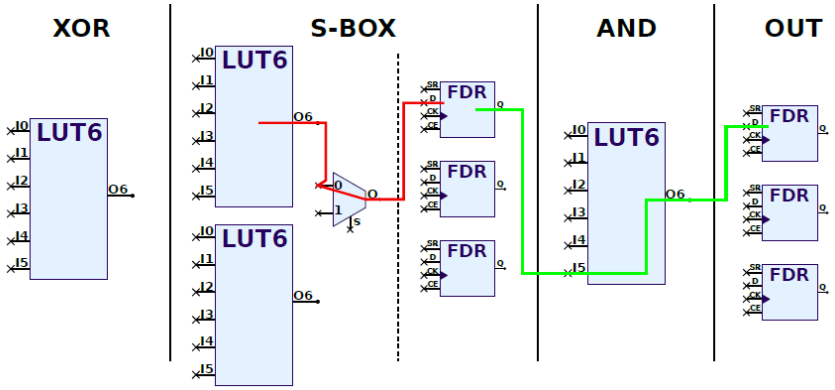
	RO_0	RO_{12}
$f_0(MHZ)$	13.58	-
$f_{max}(MHZ)$	13.72	-
Δf	+1.03%	-

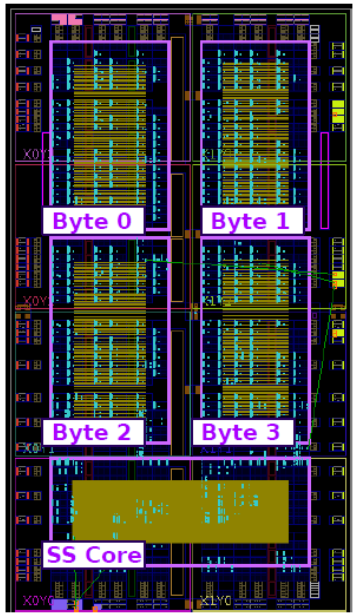
Side Channel Leakage Amplification

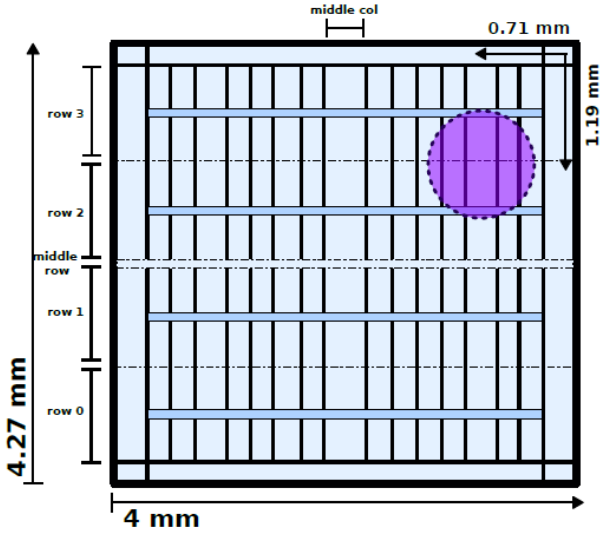
Target Architecture

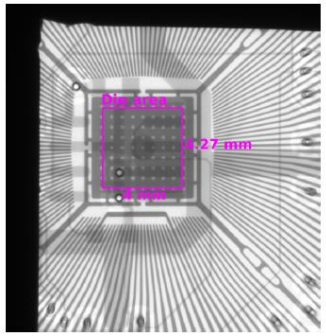
Target design and leakage paths

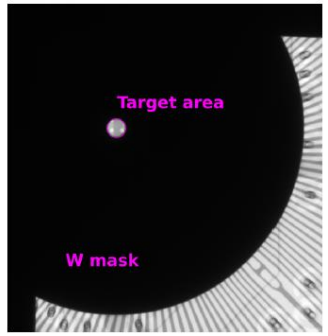




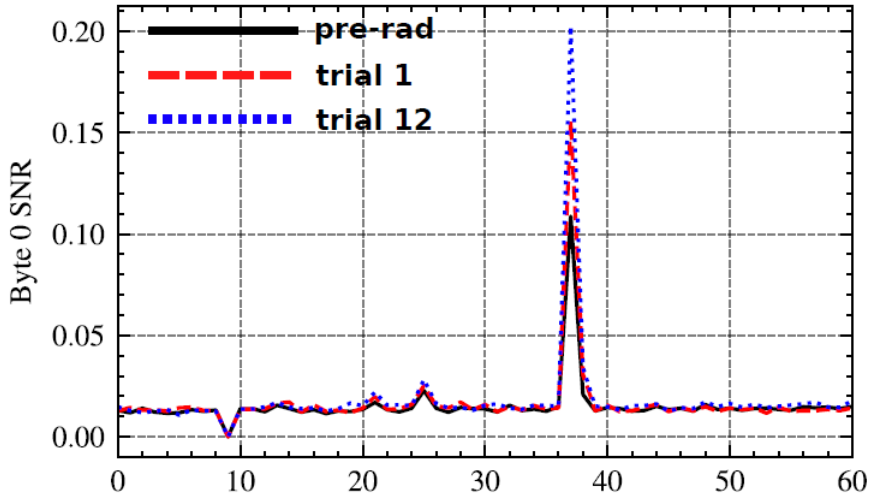


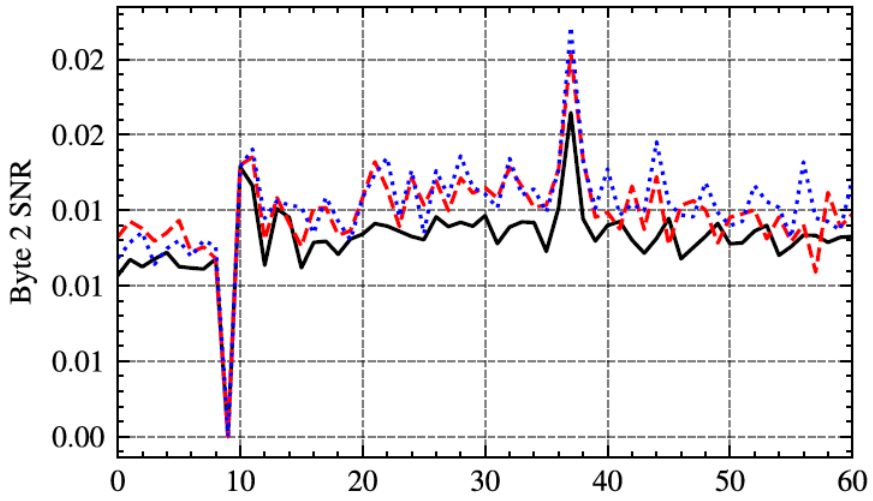




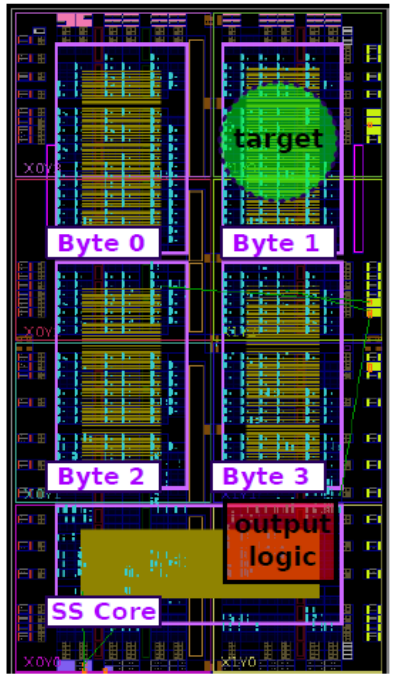


Experimental Results – SNR

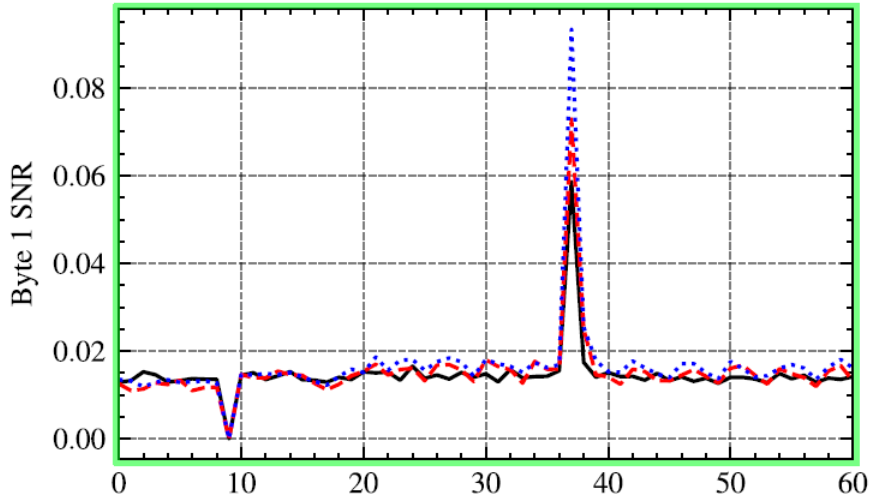


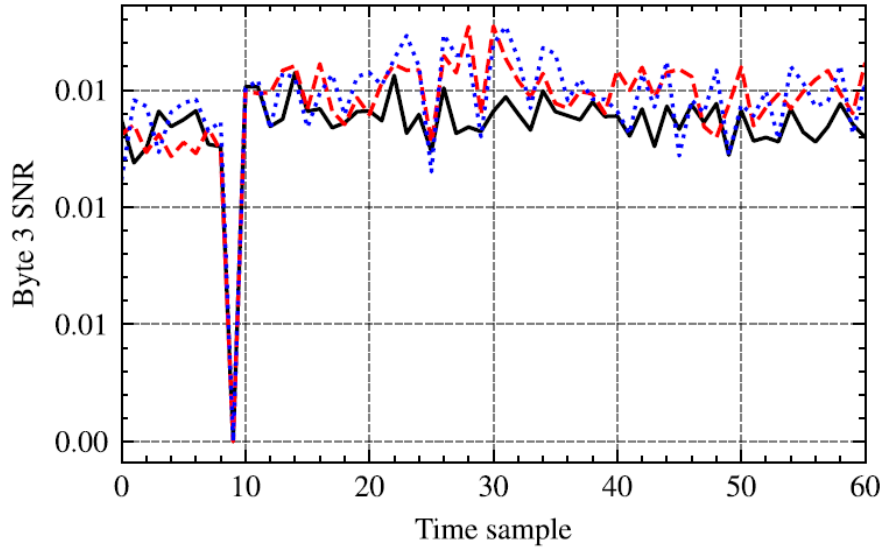


1 trial = 10 min rad

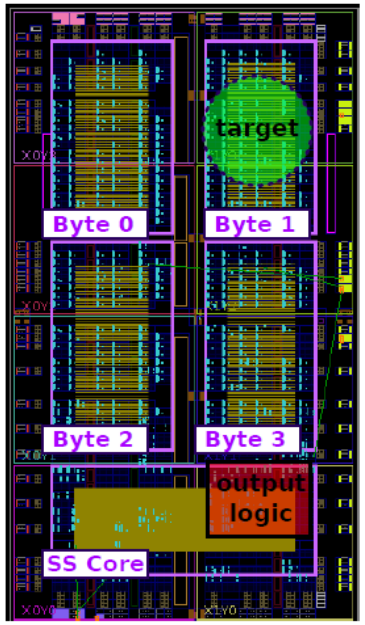


	ΔSNR_{MAX}
Byte 0	+83.7%
Byte 1	+59.2%
Byte 2	+26.5%
Byte 3	not-applicable

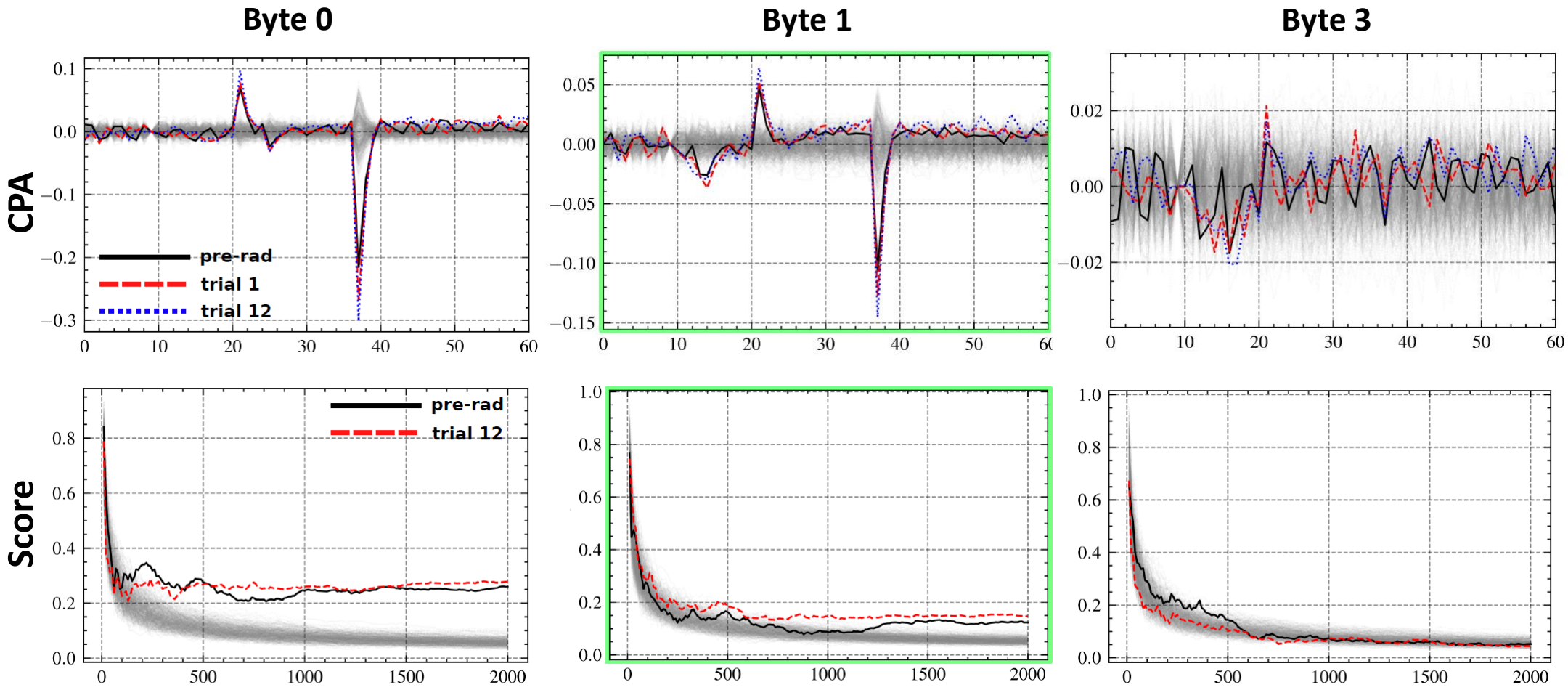




CPA & Guessing Entropy



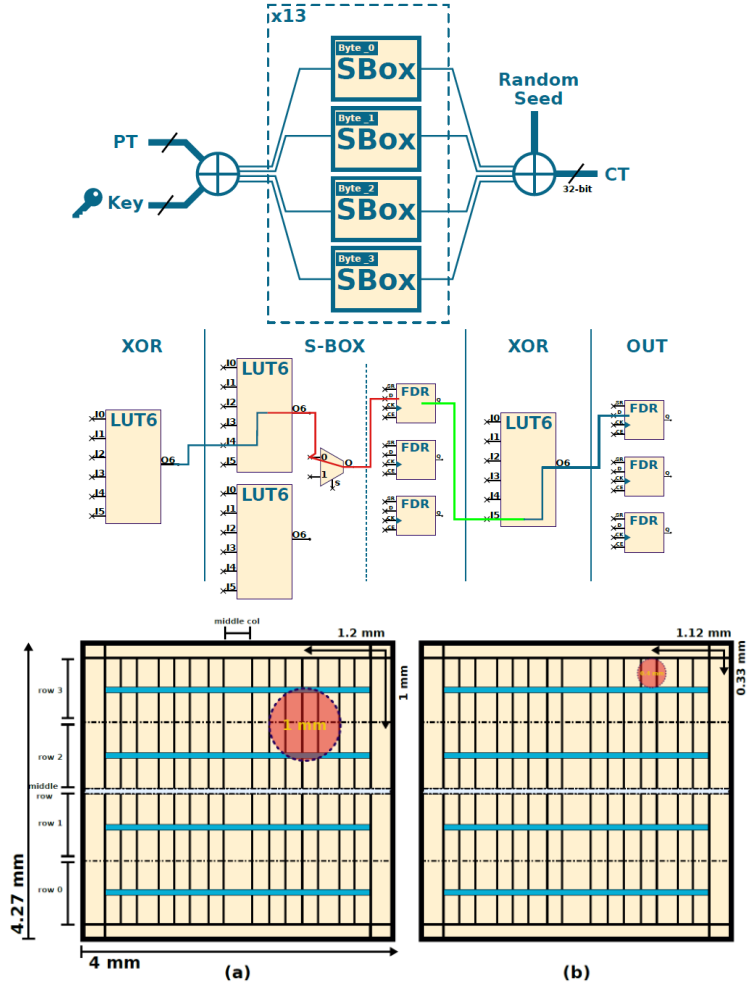
	$\Delta traces$
Byte 0	+200 (+100%)
Byte 1	-600 (-85.71%)
Byte 2	not-applicable
Byte 3	not-applicable



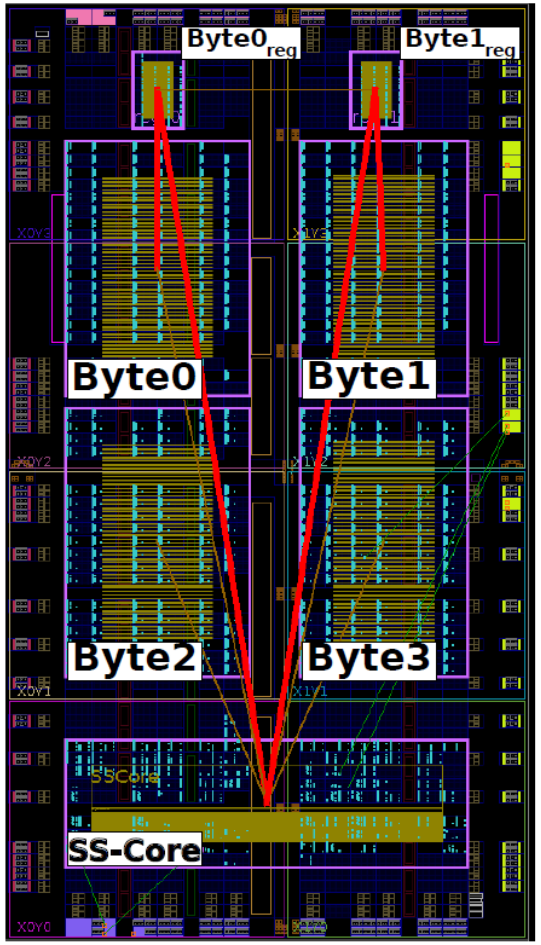
FPGA Characterization

Target Architecture

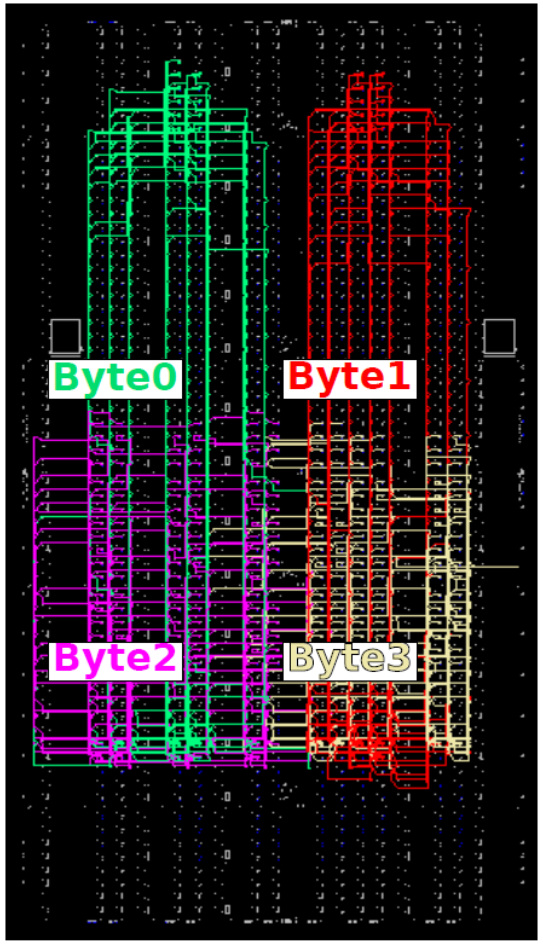
Target Architecture



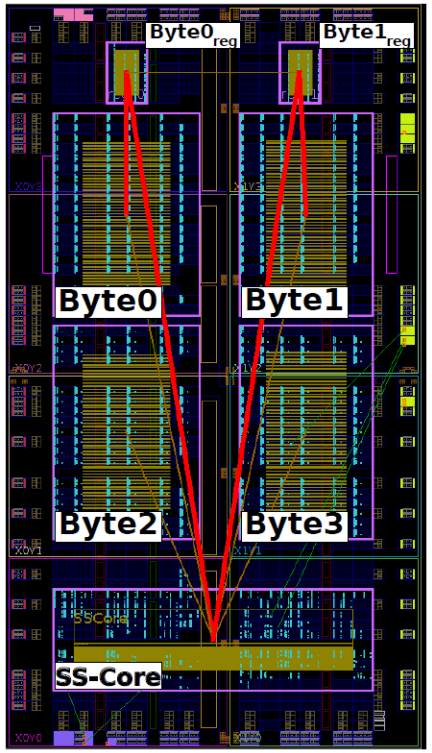
Floorplan

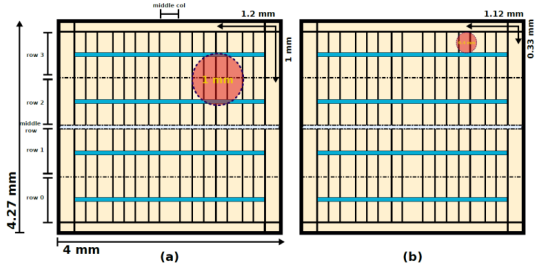


Interconnect

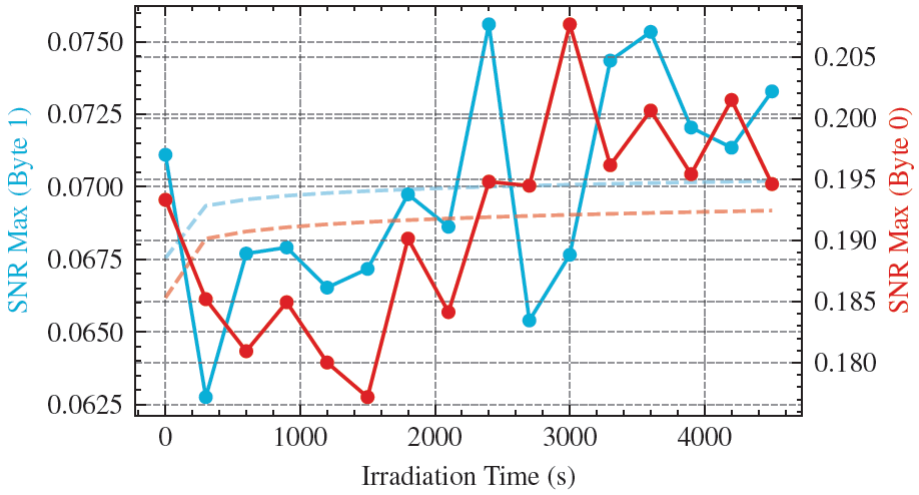


Experimental Results – SNR



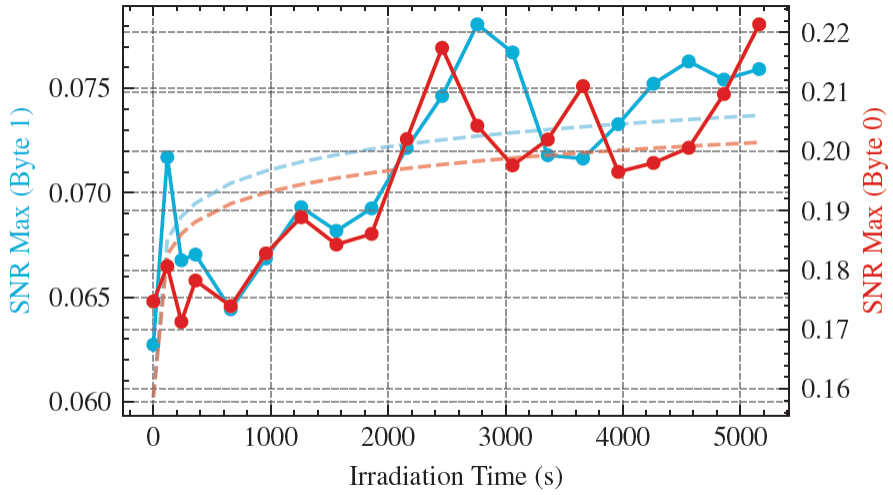


Byte-1 Combinational Irradiation



Combinational parts of the FPGA are not the main source of power consumption when compared to clocked resources

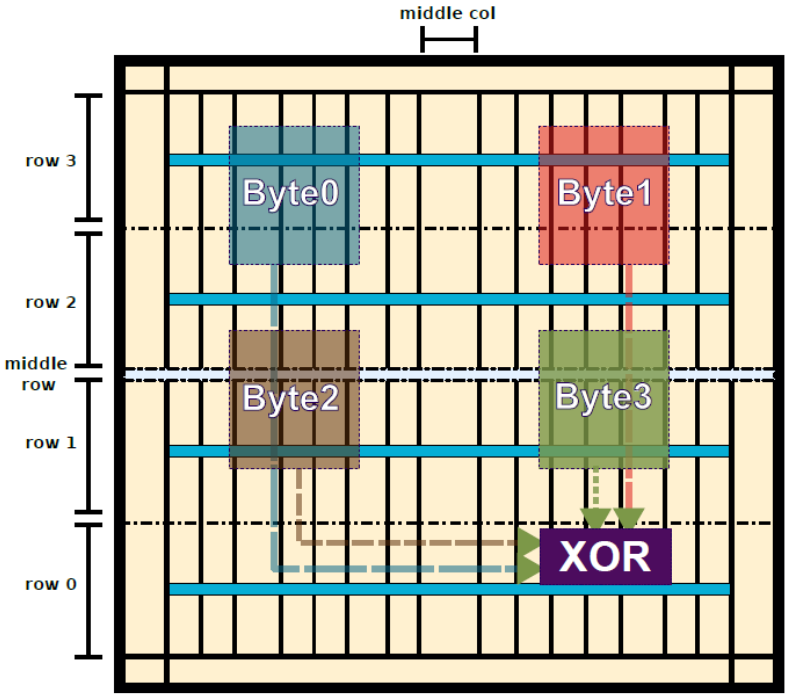
Byte-1 Register Irradiation



Registers have a higher contribution to data-dependent leakages, suggesting that registers are a better target

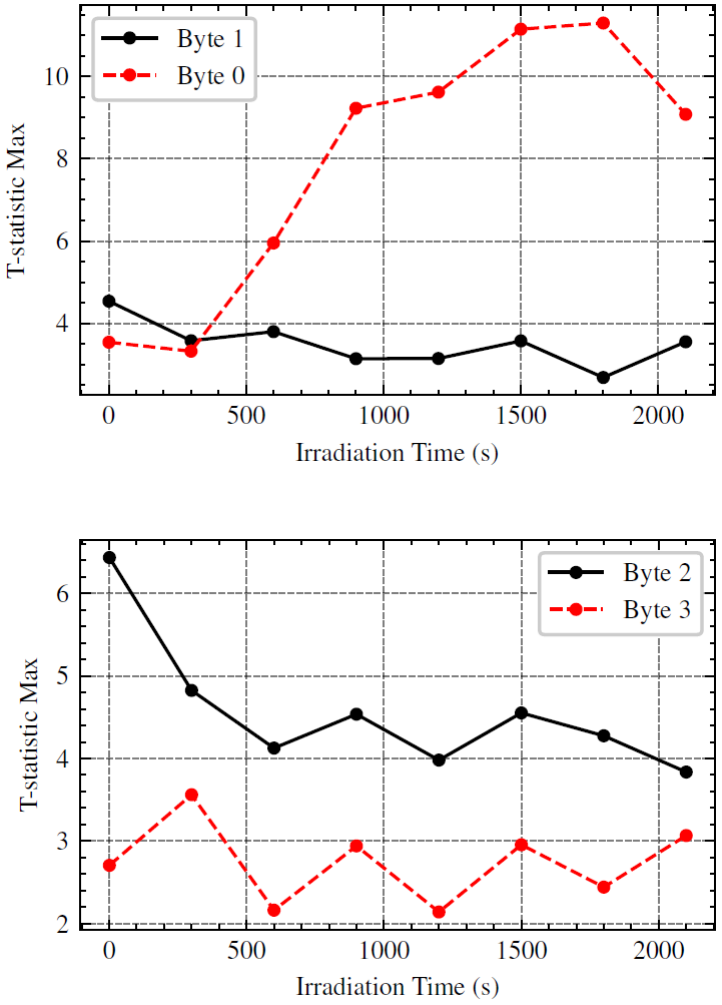
Global Irradiation Analysis

Simplified Routing Representation

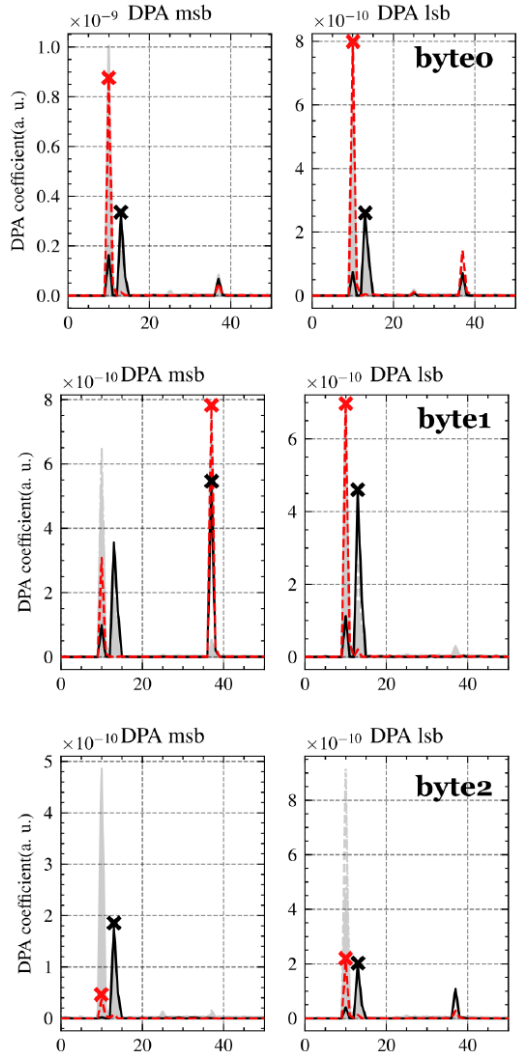


T-statistics assess **overall leakage** across two groups; DPA focuses on specific **data hypotheses**, and the correlation can improve regardless of the T-test

Welsh T-test statistic evolution



Before, After



Conclusion & Perspectives

- X-Rays attacks can be leveraged before fault occurrence
  - Side Channel leakage amplification
  - Ring Oscillator frequency biasing

- Validated through extensive experimental campaigns on FPGA
  - Real case scenarios?
  - ASIC targets ?
- Exploitability improvements?
  - Attack granularity & strength

Thanks!

Questions?