Multidimensional Strong PUF based on multifunctional thin films

Journées C2 2023
Oct. 15-20, 2023 Najac (France)

Benjamin Malthiery[1,2] (ORCID 0000-0002-4299-4467), Estelle Wagner[1] (0000-0003-4837-483X), Philippe Elbaz-Vincent[2] (0000-0002-8629-3021), Giacomo Benvenuti[1] (0000-0002-8369-636X)

1. 3D-Oxides SAS, 41 rue Henri Fabre, F-01630 Saint-Genis-Pouilly, France
2. Univ. Grenoble Alpes, CNRS, IF, 38000 Grenoble, France

Outline

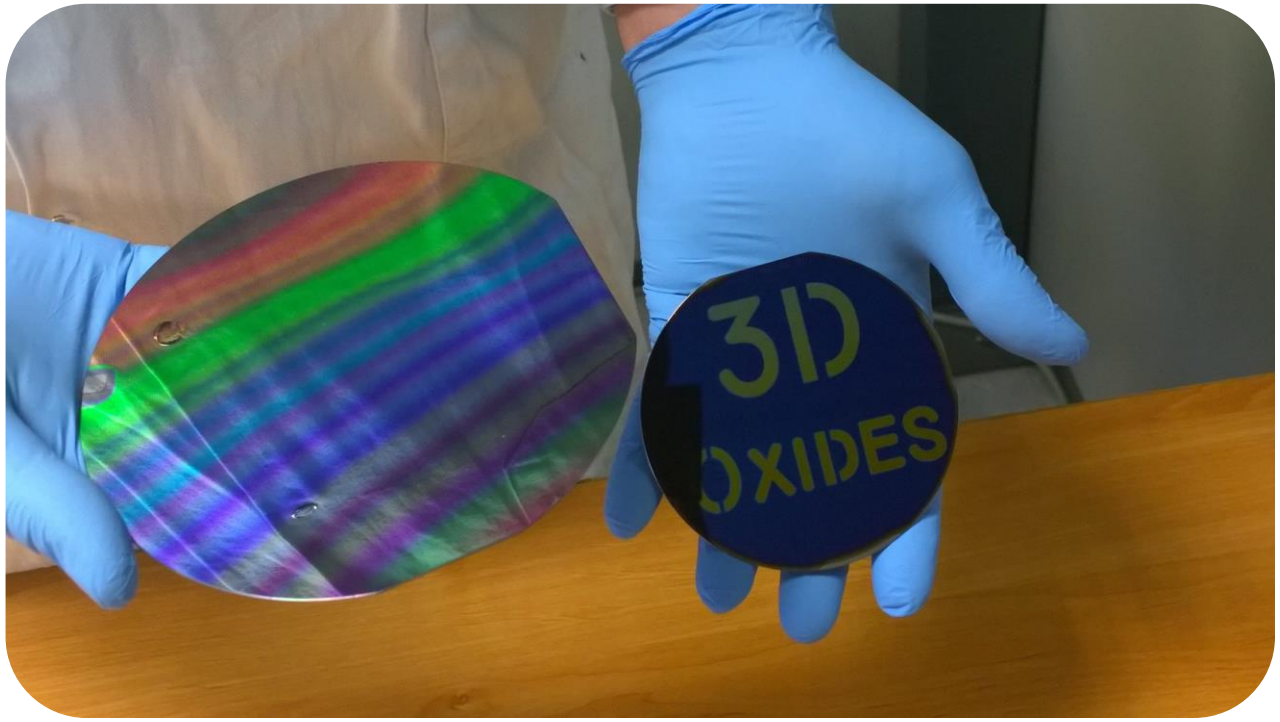
I. Introduction

II. Thesis work

Objectives

Experimental results

III. Outlook



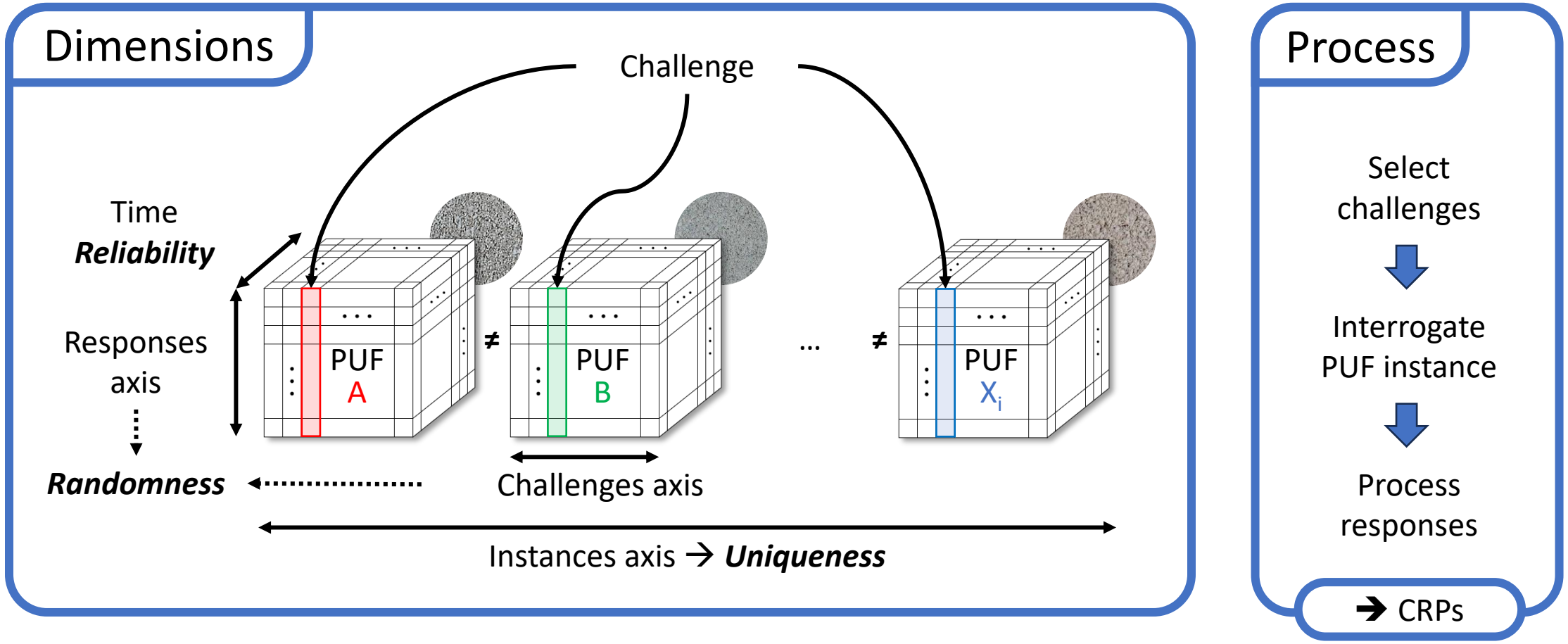
I. Introduction

- Need: combat counterfeiting and usurpation at lower cost
  - Financial losses
  - Deteriorated brand image
  - Security & Public health problem
  - Data exposed to a malicious actor

- Context: IoT growth and process automatization
- Concept: Applying biometrics to objects to provide reliable IDs at lower cost

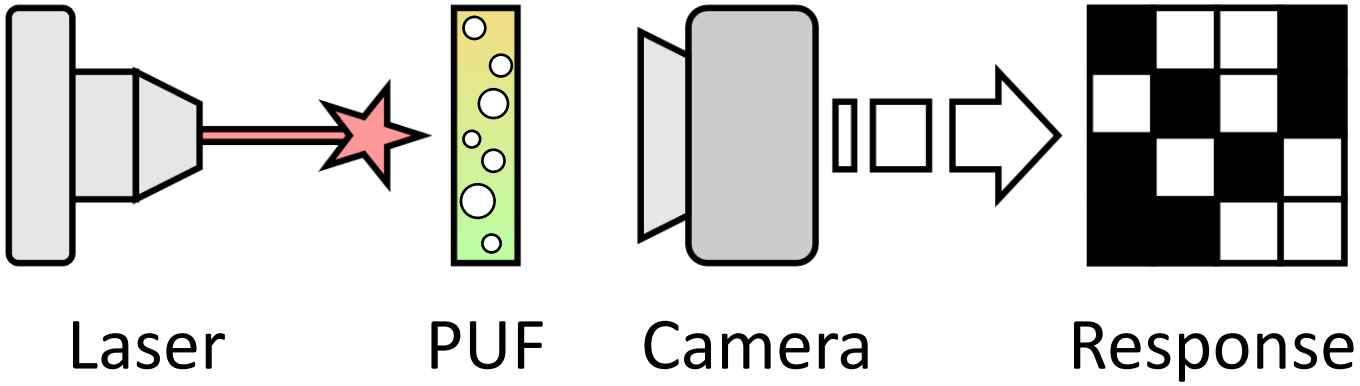
Conceptual definition

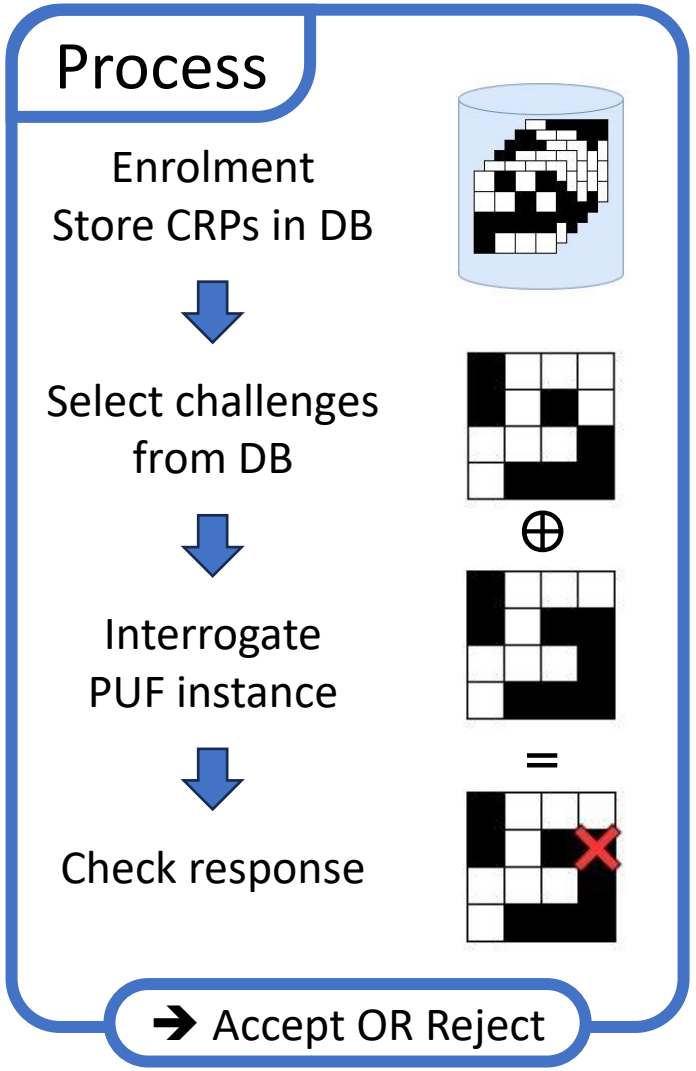
- Physical Unclonable Function (PUF) [1]



Use-cases and examples 1/2

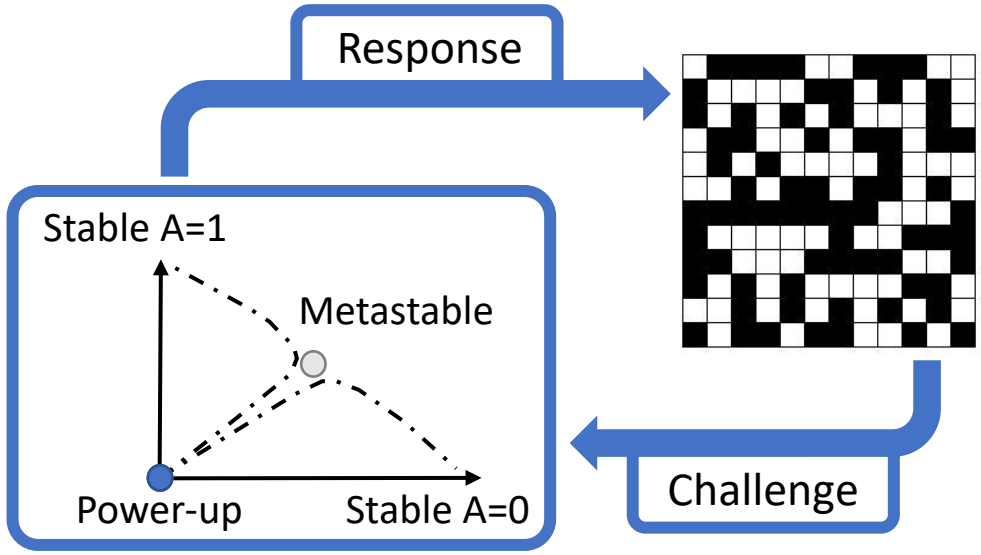
- Optical PUF & Authentication
  - Authors: Pappu et al. (2002) [2]
  - Challenge: Relative position of the laser beam
  - Response: Speckle pattern



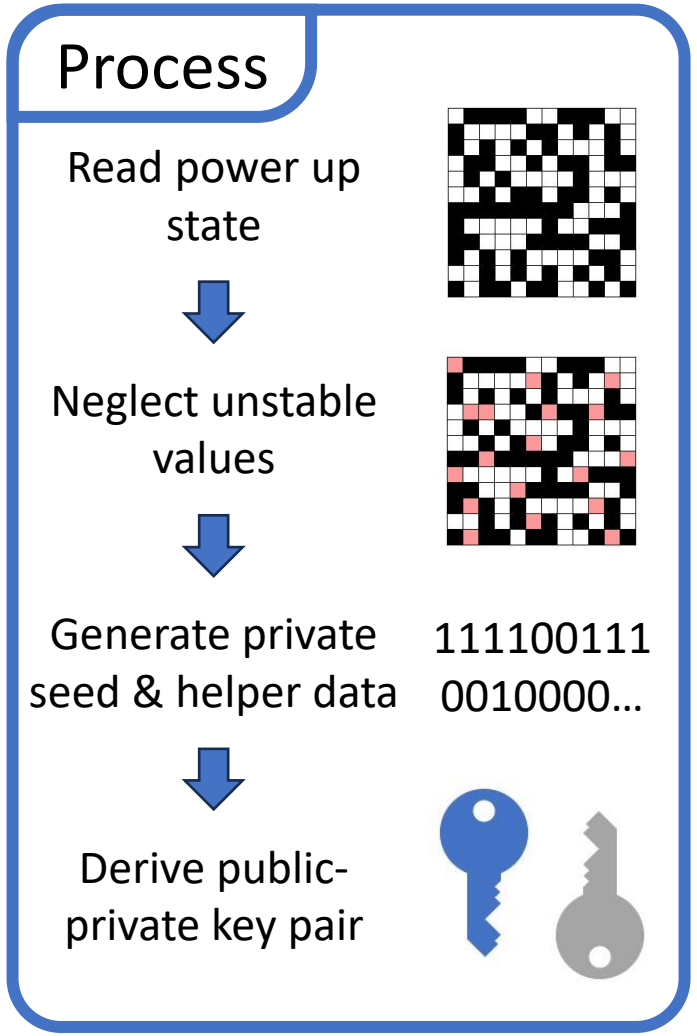


Use-cases and examples (2/2)

- SRAM PUF & Cryptographic key generation
  - Authors: Guajardo et al. (2007) [3]
  - Challenge: Position of the SRAM element
  - Response: Power up state



Power-up behavior of an SRAM cell [4][5]

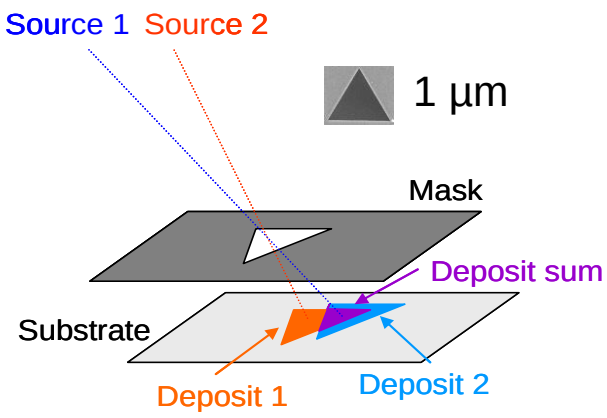


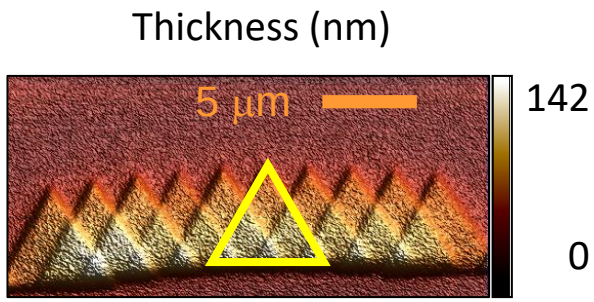
II. Thesis work – Objectives

- PUF advantages vs. Secure Elements:
  - Contained cost
  - Improved logistics by skipping key provisioning
- Identified limitations:
  - Reader cost
  - Clonability (SRAM) and modelling possibility [6]
- Project objective: Develop a new PUF design based on oxides thin films
  - Increase capacity of diversification
  - Miniaturized and integrated reader

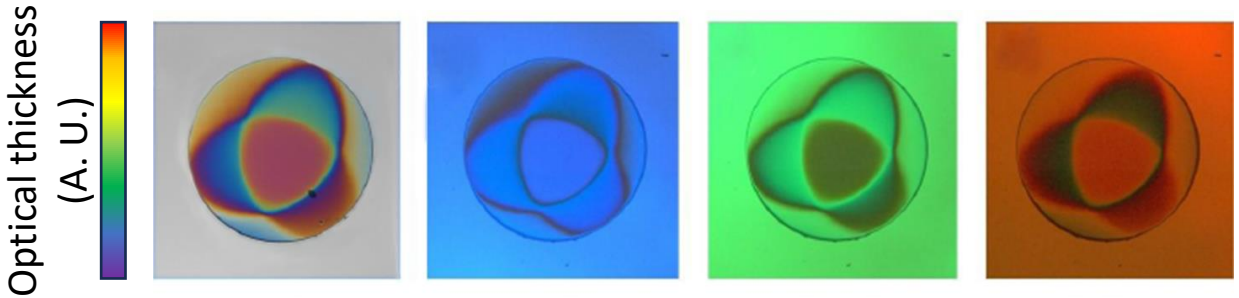
Our approach

- Multifunctional oxides thin films
  - Multi-values basis
  - Multi-properties challenges
- Theoretical challenge space: L^{Z*N}
  - L: Number of distinguishable values
  - Z: Number of stimuli/properties
  - N: Number of points
- Property: optical transmittance





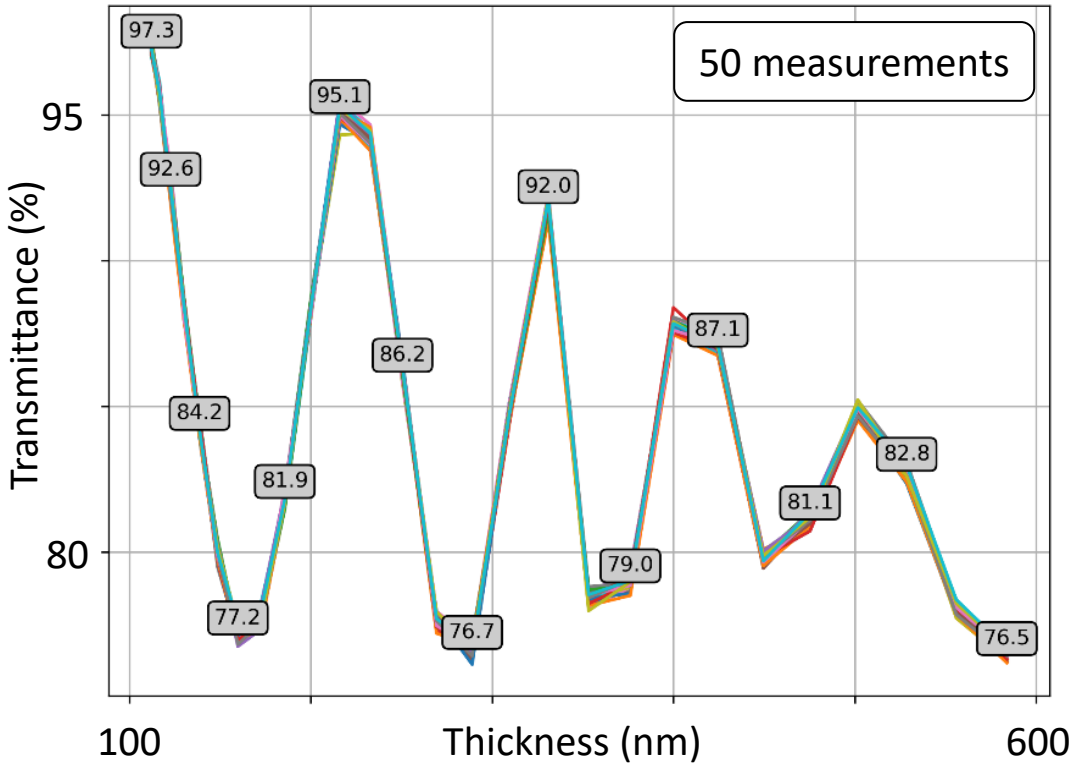
Thin film dots' thickness AFM measurement (N)

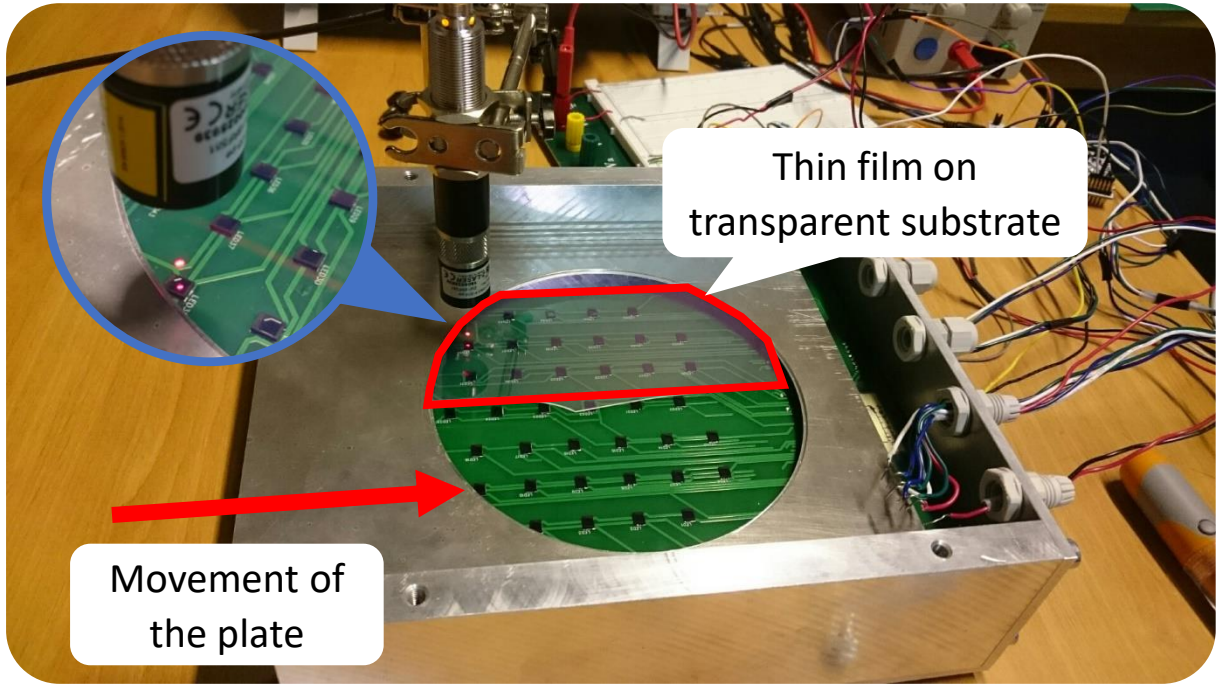


Oxides thin films reflectivity at different wavelengths (L&Z)

Experimental results – Macro PoC (1/2)

- Non-linearity of transmittance
  Thickness gradient (112 nm to 584 nm)

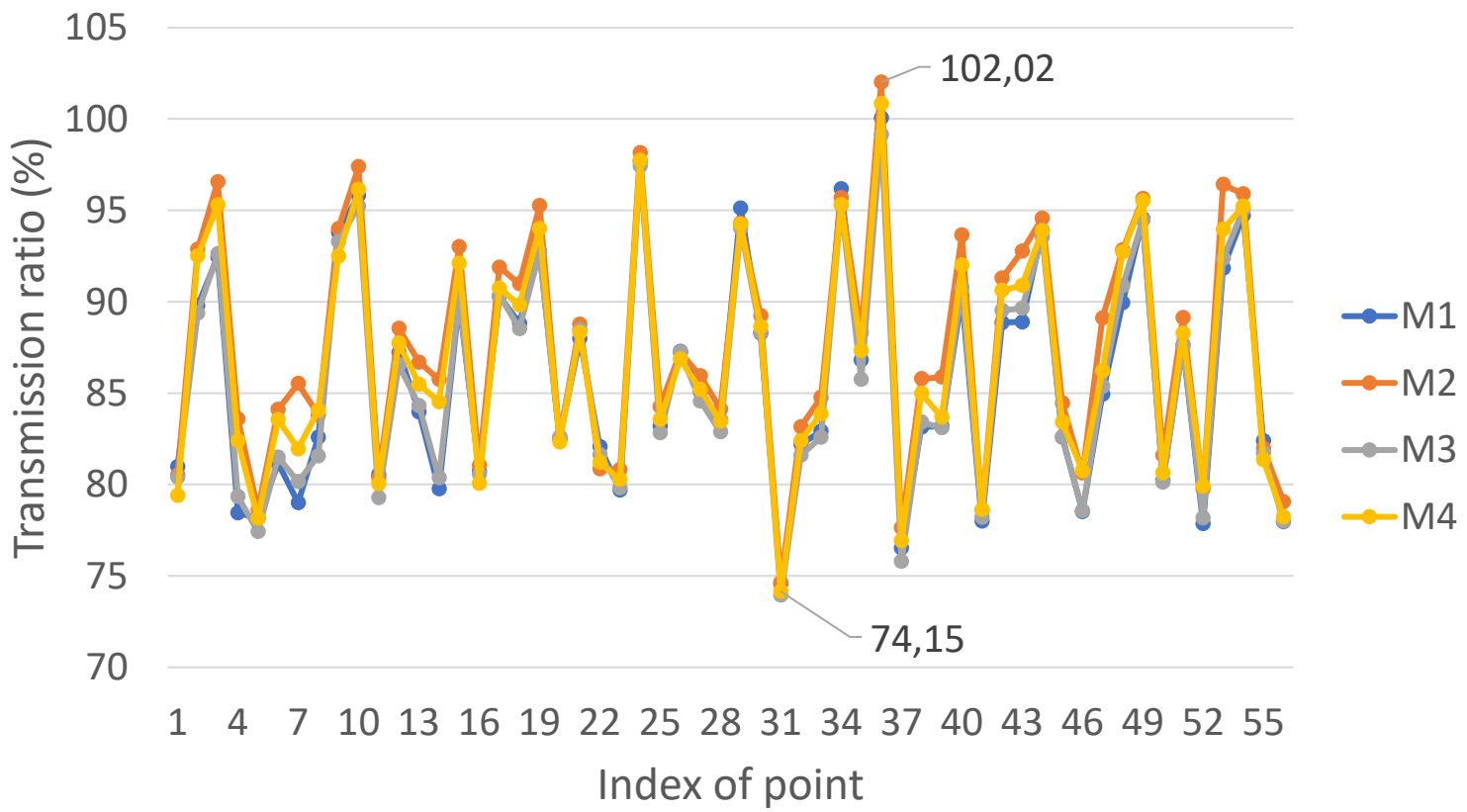


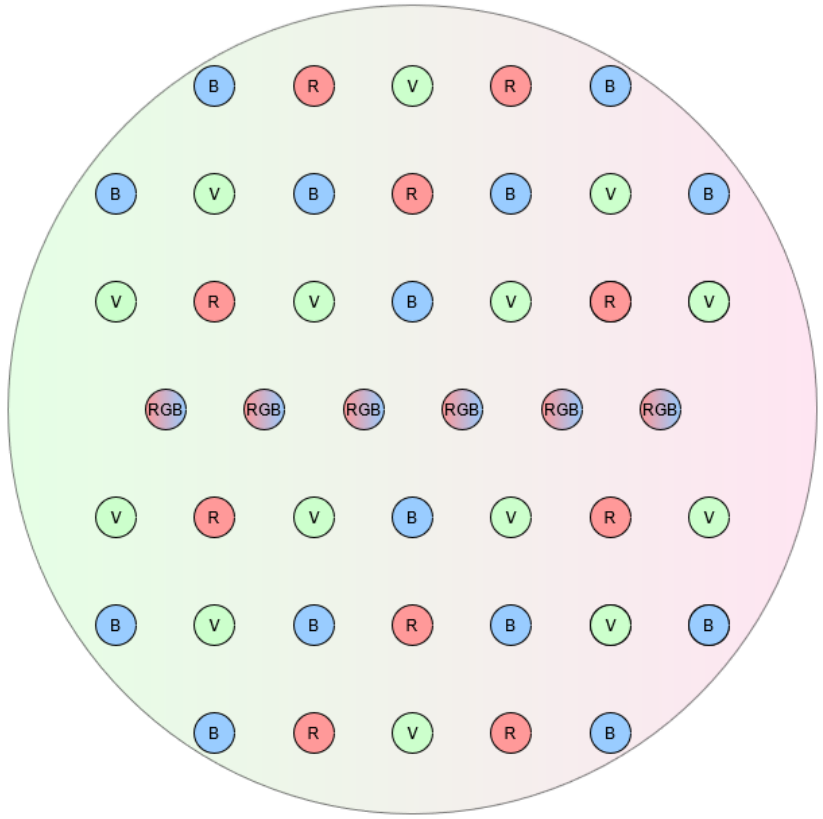


- Oscillations between 76% and 97%
- Interference effects decreases with increasing thickness (diffusion losses)

Experimental results – Macro PoC (2/2)

- Reproducibility of transmission ratio

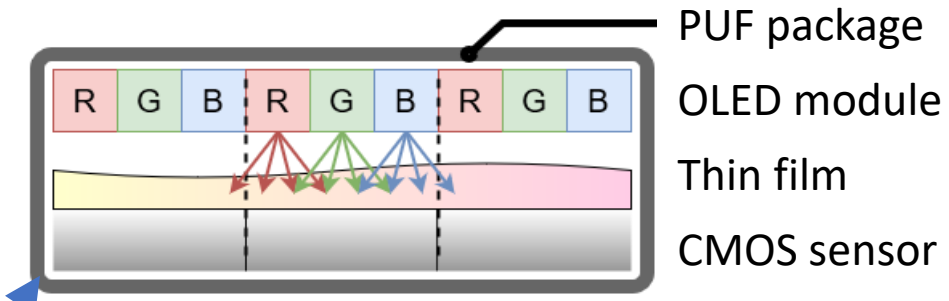




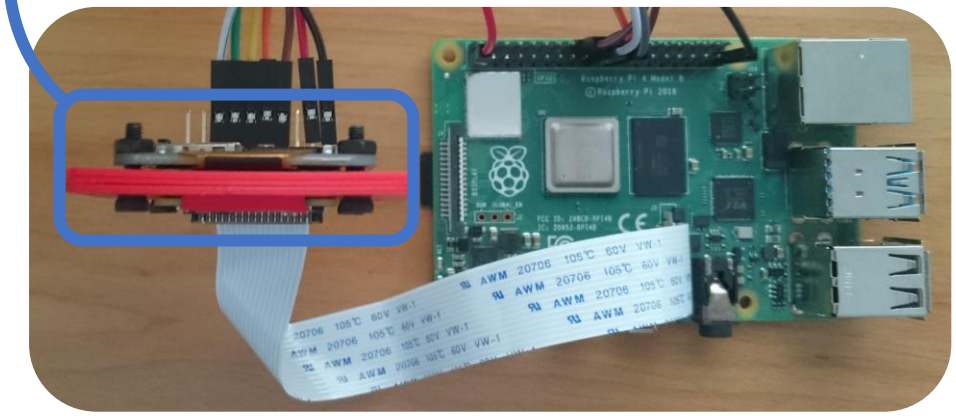
Arrangement of LED sources on the macroscopic system

Experimental results – Compact PoC (1/3)

- Shift to more compact prototype:
  - OLED display replaces LEDs
  - CMOS sensor replaces photodiodes
  - Peripherals controlled by Raspberry Pi
- Preliminary analyses:
  - RAW values & sub-pixel control



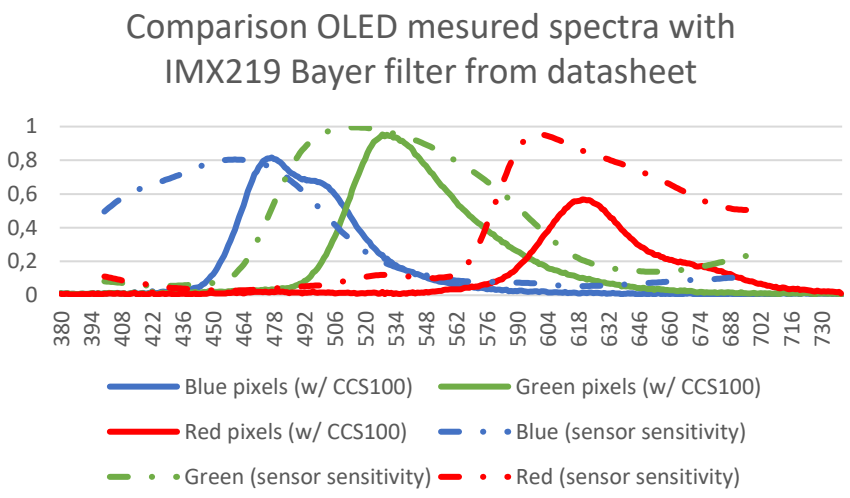
Schematic sectional view



Photograph of the experimental set-up

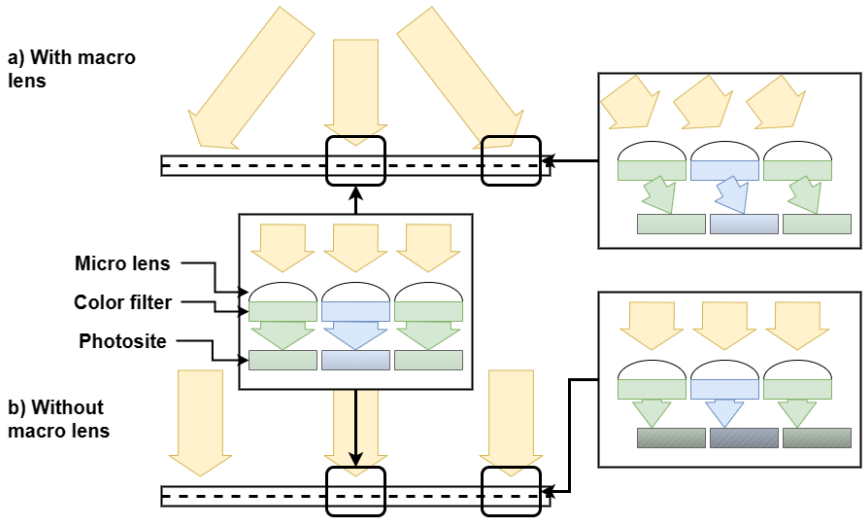
Experimental results – Compact PoC (2/3)

- Problems caused by changing components:



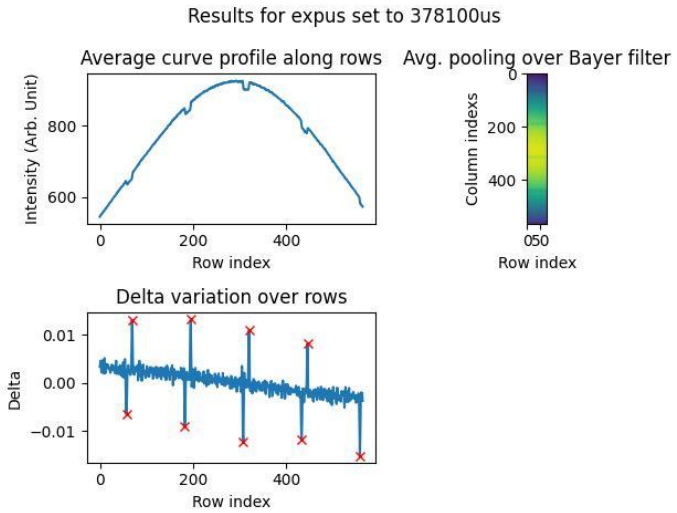
Bayer filter pattern (BGGR)

➔ Limit effect of thin film



Micro lens shifted on edges

➔ Crosstalk



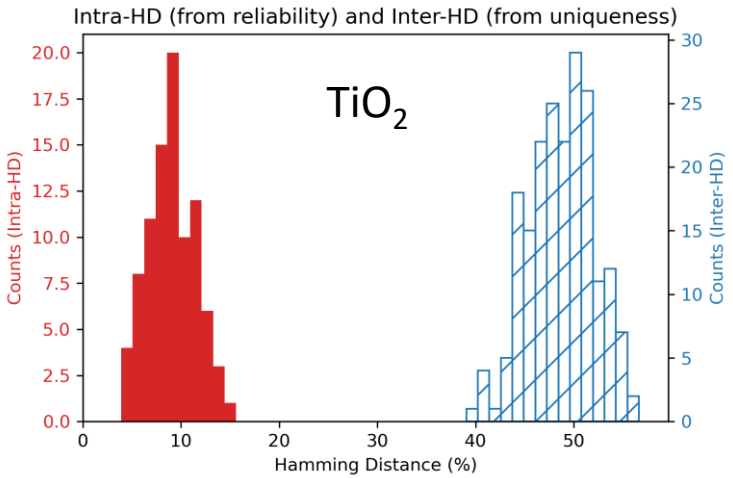
Refresh rate + Exposure time

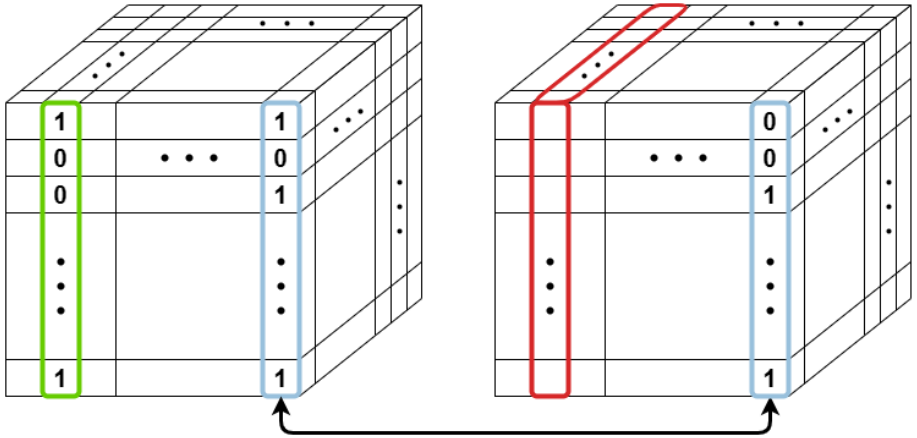
➔ Flickering phenomenon

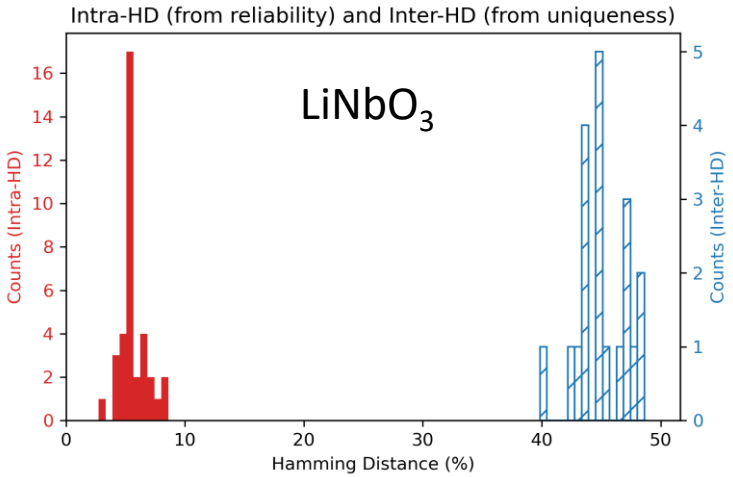
Experimental results – Compact PoC (3/3)

- Comparison of results with TiO_2 and $LiNbO_3$:

	Target	TiO_2	$LiNbO_3$
Uniformity (%)	50	51.4	48.7
Reliability (%)	100	91.1	94.5
Uniqueness (%)	50	48.5	45.0







III. Outlook

- Results confined to the experimental prototype to date
- Several avenues for progress identified:
  - Custom CMOS sensor
  - FPGA/ASIC-based reader
  - Simulation tools (noise, response discrepancy)
  - Post-processing operations

Thank you for your attention

References

- [1] Maiti, Abhranil, Vikash Gunreddy, et Patrick Schaumont. « A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions ». In *Embedded Systems Design with FPGAs*, édité par Peter Athanas, Dionisios Pnevmatikatos, et Nicolas Sklavos, 245-67. New York, NY: Springer, 2013. https://doi.org/10.1007/978-1-4614-1362-2_11.
- [2] Pappu, Ravikanth, Ben Recht, Jason Taylor, et Neil Gershenfeld. « Physical One-Way Functions ». *Science* 297, nº 5589 (20 septembre 2002): 2026-30. https://doi.org/10.1126/science.1074376.
- [3] Guajardo, Jorge, Sandeep S. Kumar, Geert-Jan Schrijen, et Pim Tuyls. « FPGA Intrinsic PUFs and Their Use for IP Protection ». In *Cryptographic Hardware and Embedded Systems - CHES 2007*, édité par Pascal Paillier et Ingrid Verbauwhede, 63-80. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2007. https://doi.org/10.1007/978-3-540-74735-2_5.
- [4] Maes, Roel. *Physically Unclonable Functions: Constructions, Properties and Applications*. *Physically Unclonable Functions: Constructions, Properties and Applications*. Vol. 9783642413957, 2013. https://doi.org/10.1007/978-3-642-41395-7.
- [5] Zhang, Shen, Bin Gao, Dong Wu, Huaqiang Wu, et He Qian. « Evaluation and Optimization of Physical Unclonable Function (PUF) Based on the Variability of FinFET SRAM ». In *2017 International Conference on Electron Devices and Solid-State Circuits (EDSSC)*, 1-2. Hsinchu: IEEE, 2017. https://doi.org/10.1109/EDSSC.2017.8126474.
- [6] Helfmeier, Clemens, Christian Boit, Dmitry Nedospasov, et Jean-Pierre Seifert. « Cloning Physically Unclonable Functions ». In *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 1-6, 2013. https://doi.org/10.1109/HST.2013.6581556.

Supplementary Information

Process exploiting local maxima of transmission factor

Acquisitions without thin film → Acquisitions with thin film sample → Calculate transmission factors → Define responses → Analyze responses

- Challenge
  - OLED pixel position
  - Sub-pixel color
  - Sensor pixel position
- Response
  - Binary value