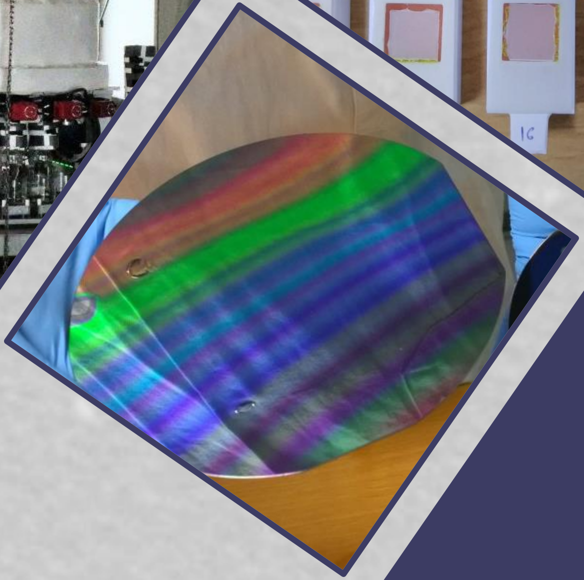
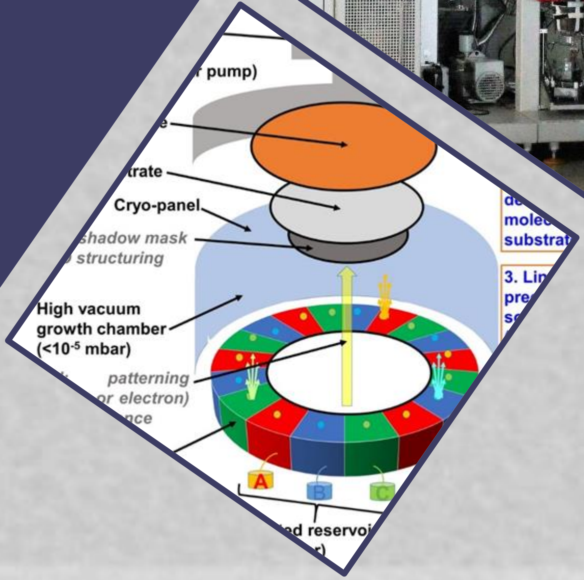
Physical Unclonable Function based on multifunctional oxide thin films

Benjamin Malthiery
3D-Oxides

European Cyber Week 2024





SU3800 3.00kV 5.1mm x7.50k SE
5.00µm

Outline

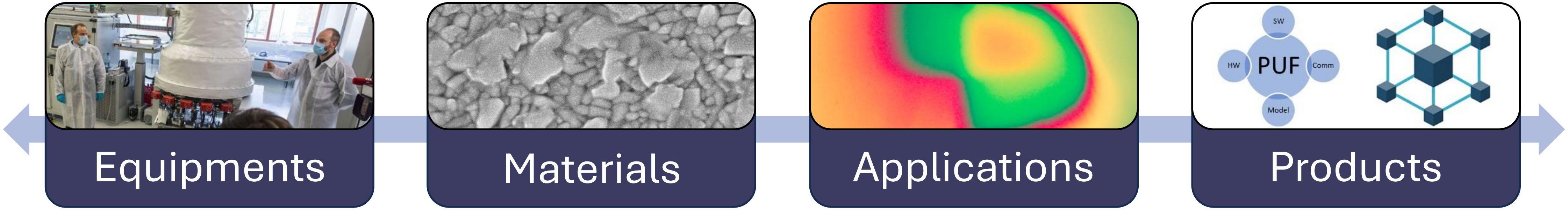
1. Project context
2. Company proposition and related works
3. Systems considered
4. Results and Discussion
5. Conclusion and Outlook

1. Project context

Backgrounds on thin films & deposition techniques

Company presentation

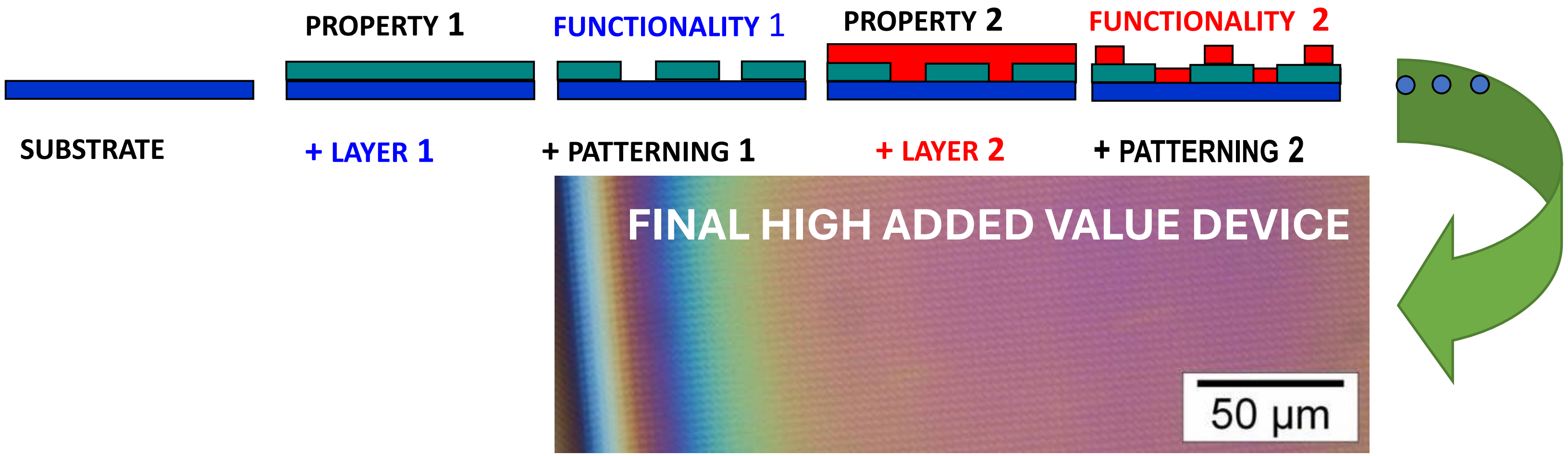
- French SME incorporated in 2009
- On the border with Switzerland (Geneva)
- Expertise in chemical precursors synthesis, thin films, and materials science



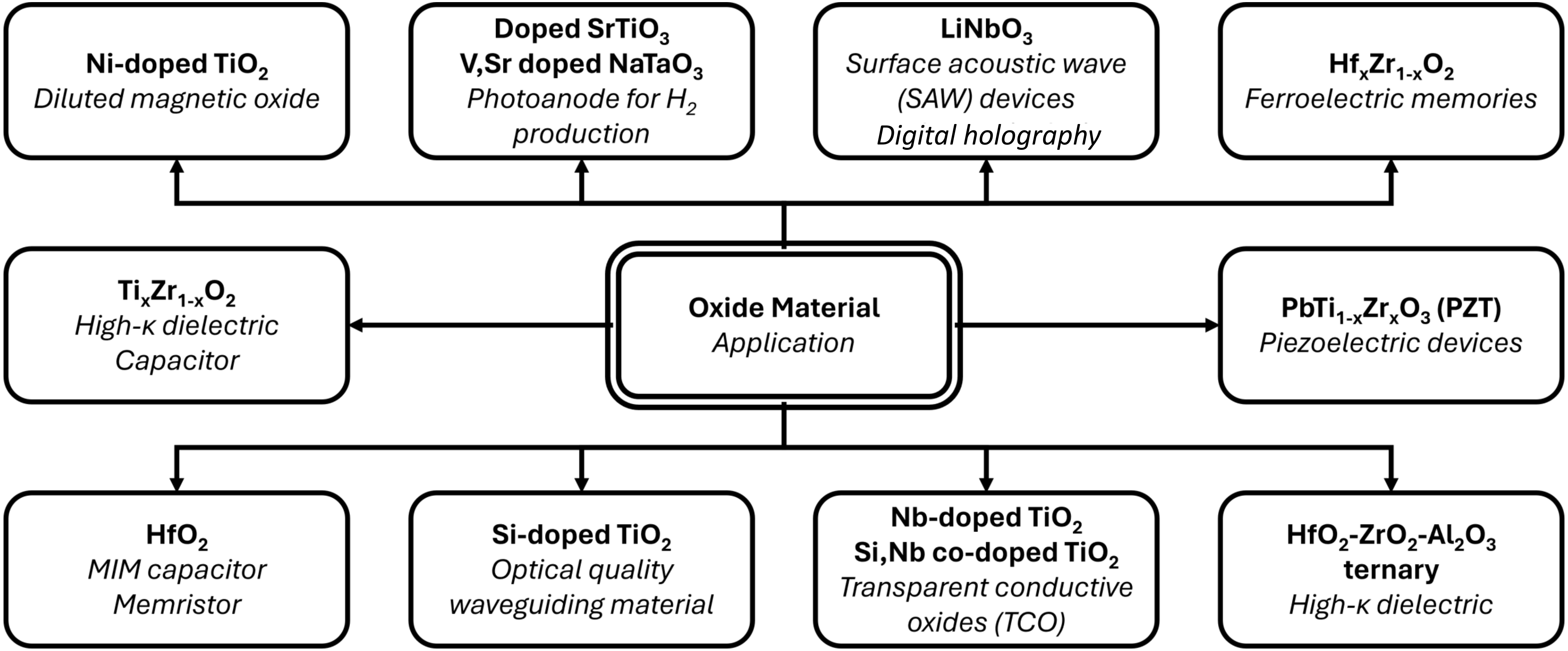
- Focused on R&D for novel materials with optimized properties
- Can provide either uniform coatings or with controlled gradients in either thickness (single element) or composition (multi elements)

Thin films definition

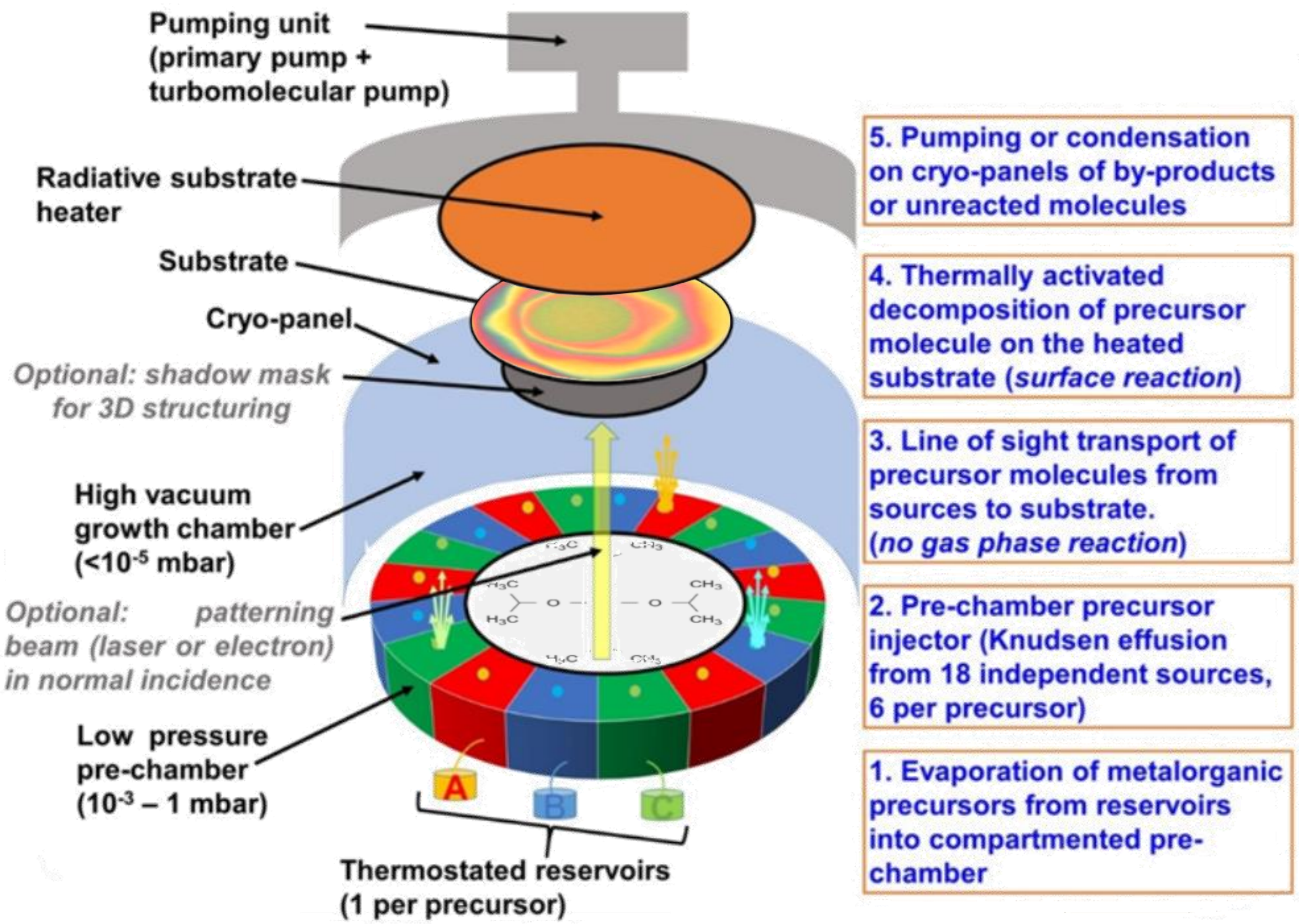
- High-tech layers with thickness from 10 nm to 10 µm allowing:
  - Miniaturization of devices
  - Development of new material (properties due to nano-size effects)
  - Integration of new functionalities (value) onto a substrate
- Sustainability: More functionalities with less resources



Thin films applications



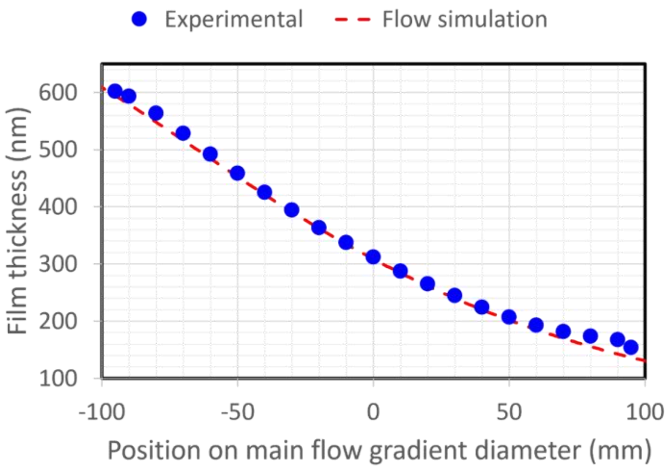
Chemical Beam Vapor Deposition

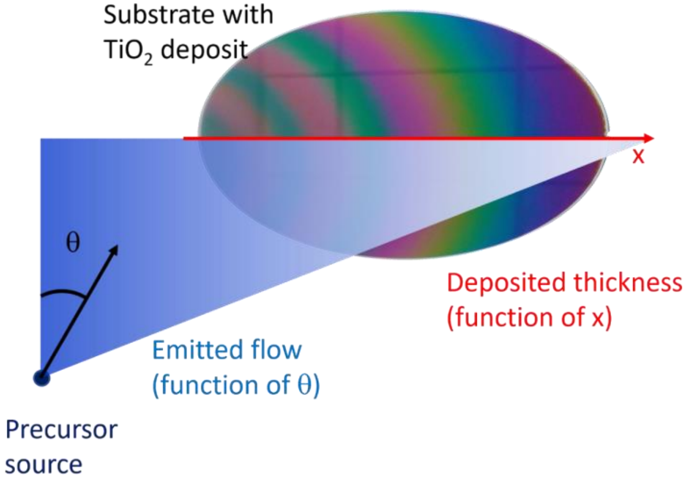


Equipment Sybilla 200

Technical background on CBVD

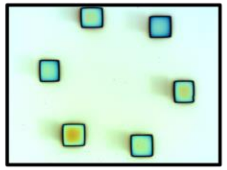
Combinatorial deposition

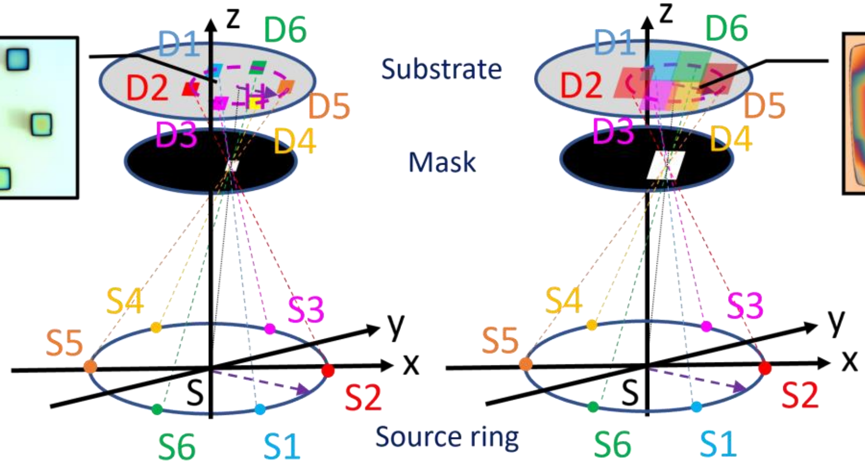


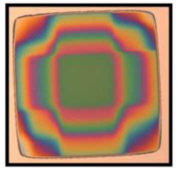


Patterning depositing through shadow mask

Separated deposits







Superposed deposits

2. Company proposition and related works

Twin PUF based on thin films

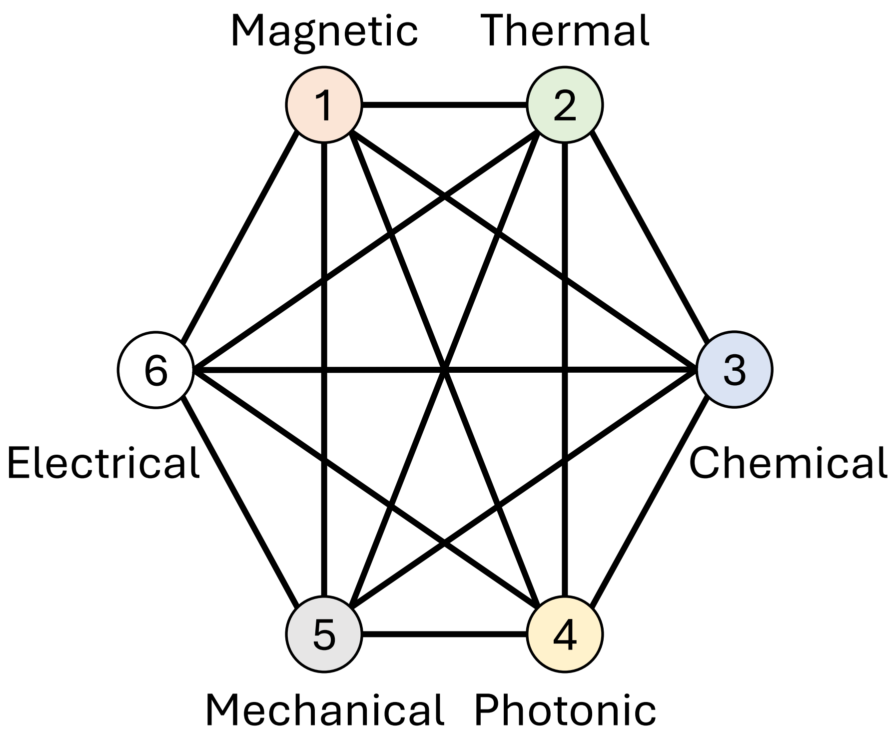
Project context

- Products to address new markets:
  - Patterned logo for luxury companies
  - Anti-counterfeiting tags
  - Physical Unclonable Functions
- Project objective: Develop a new Strong PUF construction
  - High capacity of diversification
  - Miniaturization and integration (with intrinsic evaluation)
- Differentiation:
  - Based on complex 3D nano-materials properties
  - Twin-PUF Hardware database

Interest of multifunctional thin films

- Multifunctional oxides thin films by CBVD
  - Multi-values basis
  - Multi-properties challenges
- Theoretical challenge space: $L^{Z \times N}$
  - L: Number of distinguishable values
  - Z: Number of stimuli/properties
  - N: Number of points

→ Oxide thin film PUF (OTF-PUF)



Categories of PUF [1]

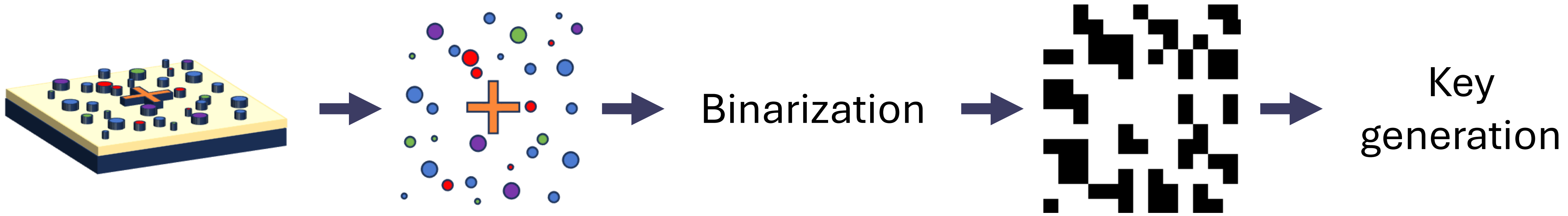
Electronic			Hybrid		
Time	Memory	Others	Optical	RF	Taggants
Arbiter PUF (delay)	Memristor PUF (HRS/LRS)	Coating PUF (C)	Optical PUF (intensity)	LC PUF (power absorbed)	Chemical PUF (presence)

⋮

[1] McGrath, Thomas, Ibrahim E. Bagci, Zhiming M. Wang, Utz Roedig, and Robert J. Young. "A PUF taxonomy". Applied Physics Reviews 6, n° 1 (2019): 011303. https://doi.org/10.1063/1.5079407.

Physico-chemical PUF

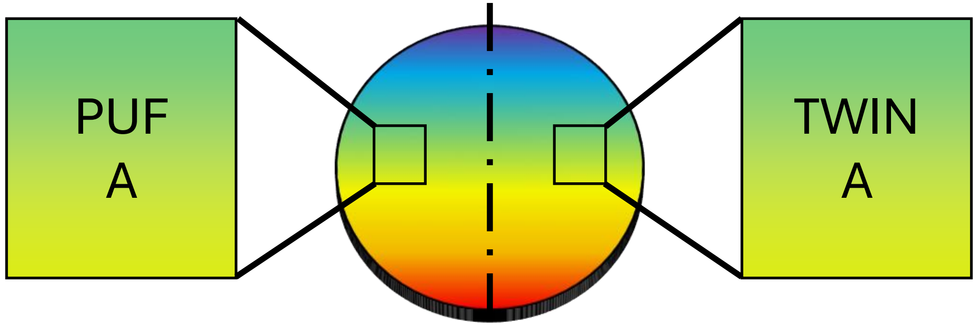
- Physico-chemical PUF [2] & Thin films PUF [3]
- Challenge: Sample area and/or Chemical method
- PUF: Physical properties of materials
- Response: Presence or absence of taggants



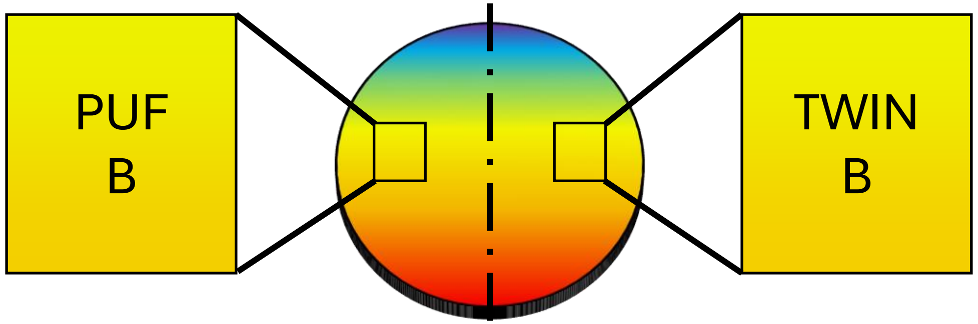
[2] Arppe, Riikka, et Thomas Just Sørensen. “Physical Unclonable Functions Generated through Chemical Methods for Anti-Counterfeiting”. *Nature Reviews Chemistry* 1, nº 4 (2017): 1-13. https://doi.org/10.1038/s41570-017-0031.
[3] Torun, Neslihan, Ilker Torun, Menekse Sakir, Mustafa Kalay, et M. Serdar Onses. “Physically Unclonable Surfaces via Dewetting of Polymer Thin Films”. *ACS Applied Materials & Interfaces* 13, nº 9 (2021): 11247-59. https://doi.org/10.1021/acsami.0c16846.

Twin PUF

- PUF and Twin sharing a certain degree of similarity
  - Points symmetrical about the gradient axis
  - Neighboring thin film zones
- Twin is not a Clone / Duplicate
  - Different scales of precision (mm/µm/nm)
  - Additional altering step (laser)
- Pros: Skip enrolment & Benefit from larger CRP space
- Cons: Constraints on calibration & Management of physical twins in DB



Sample A (PUF A ≈ TWIN A)



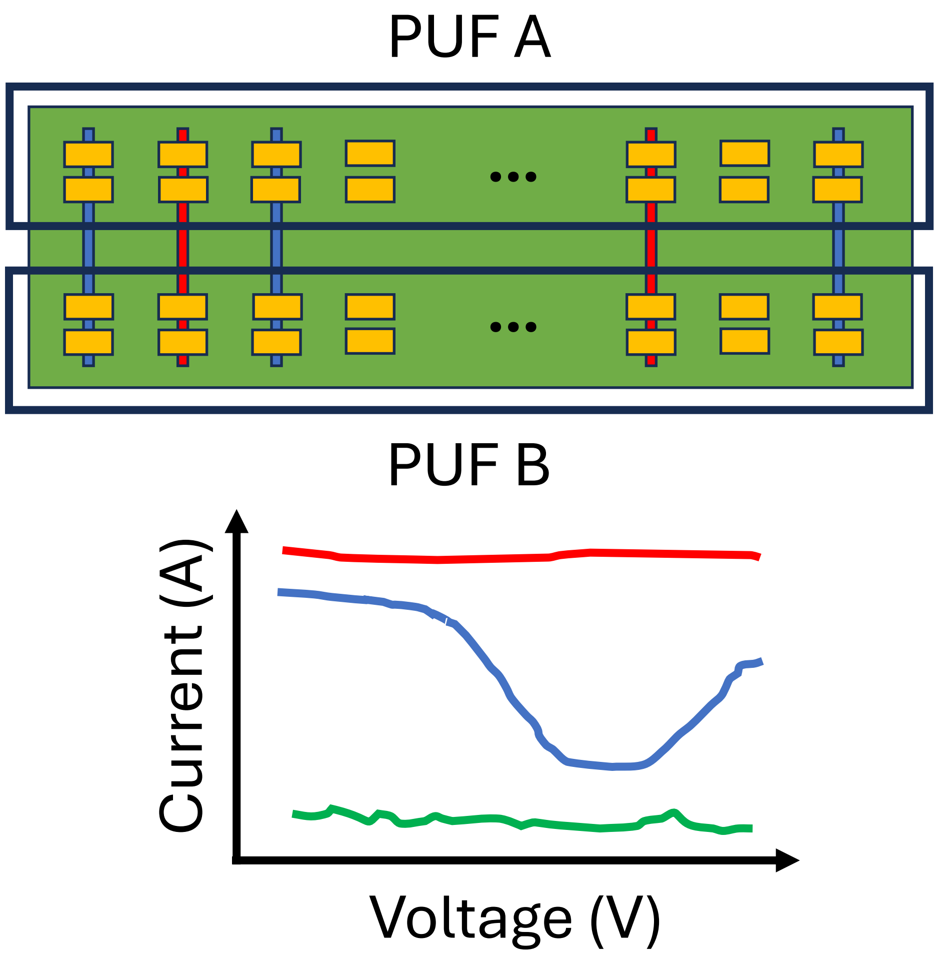
Sample B (PUF B ≈ TWIN B)

Carbon Nanotube Arrays Twin PUF

- Carbon Nanotubes PUF [4]
- Challenge: CNFET position
- PUF: CNFET chirality & position
- Response: Nanotube conductivity
- 2 identical PUFs in 1 fabrication run

→ Communication without enrolment or DB storage

Fully similar, unlike our solution



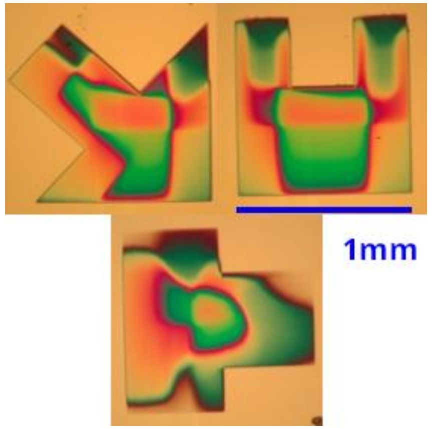
[4] Zhong, Donglai, Jingxia Liu, Mengmeng Xiao, Yunong Xie, Huiwen Shi, Lijun Liu, Chenyi Zhao, Li Ding, Lian-Mao Peng, et Zhiyong Zhang. “Twin Physically Unclonable Functions Based on Aligned Carbon Nanotube Arrays”. *Nature Electronics* 5, nº 7 (2022): 424-32. https://doi.org/10.1038/s41928-022-00787-x.

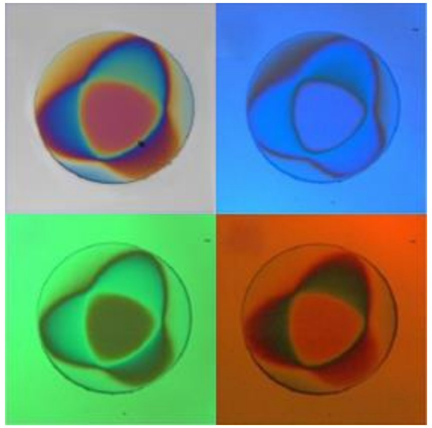
3. Systems considered

Evaluated properties and prototypes

System considered

- Based on thin films optical transmittance → OTFT-PUF
- Advantages
  - Typically transparent
  - Impacted by thin film composition and morphology
  - Several simulation models in the literature [5, 6]
  - Easier to evaluate
- Bottlenecks for integration
  - Dynamic range of sensor
  - Signal-to-noise ratio



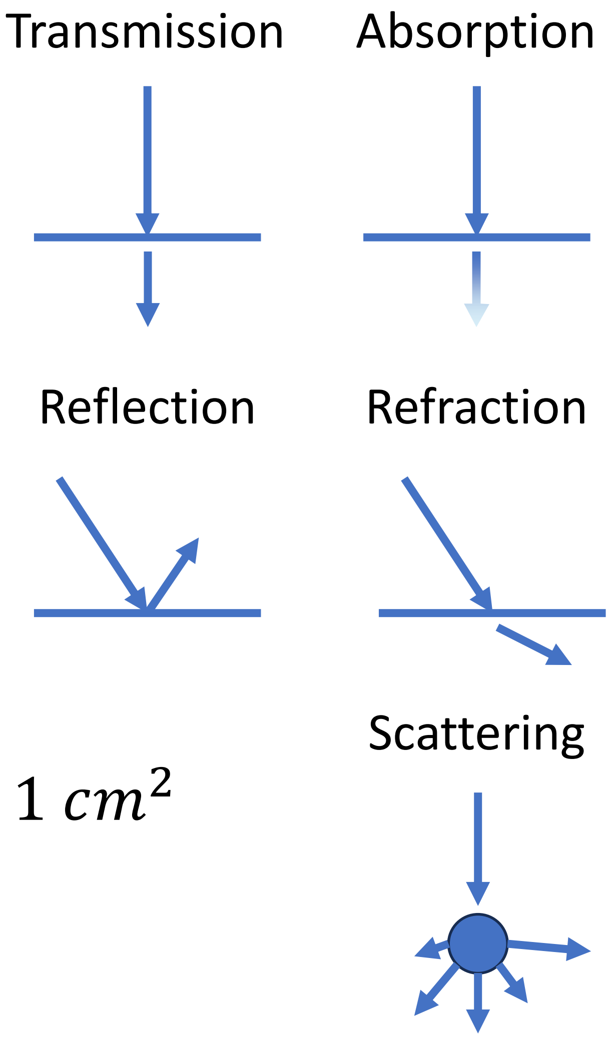


[5] Tomlin, S. G. "Optical Reflection and Transmission Formulae for Thin Films". Journal of Physics D: Applied Physics 1, n° 12 (December 1968): 1667. https://doi.org/10.1088/0022-3727/1/12/312.
[6] Swanepoel, R. "Determining Refractive Index and Thickness of Thin Films from Wavelength Measurements Only". JOSA A 2, n° 8 (August 1, 1985): 1339-43. https://doi.org/10.1364/JOSAA.2.001339.

Targeted PUF

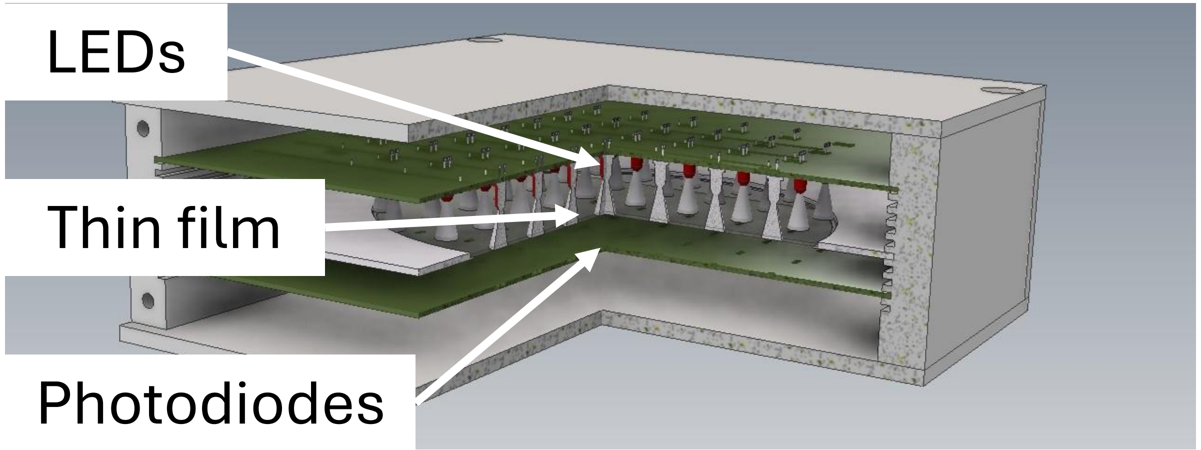
- Parameters
  - L: Number of values (based on sensor bit-depth)
  - Z: Number of stimuli (emission spectra, intensity, λ, θ)
  - N: number of points (thin film lateral resolution)
- Capacity of diversification
  - L = 10^3 (10 bits)
  - Z = 10^6 (100 intensity levels on 3 channels)
  - N = 10^8 (dot of 1 μm^2 on 1 cm^2)

  → $L^{Z \times N} = 10^{3 \times 10^6 \times 10^8} = 10^{3 \times 10^{14}} \approx 2^{2^{49}}$ *combinations on* $1\ cm^2$
- Could be increased by other properties



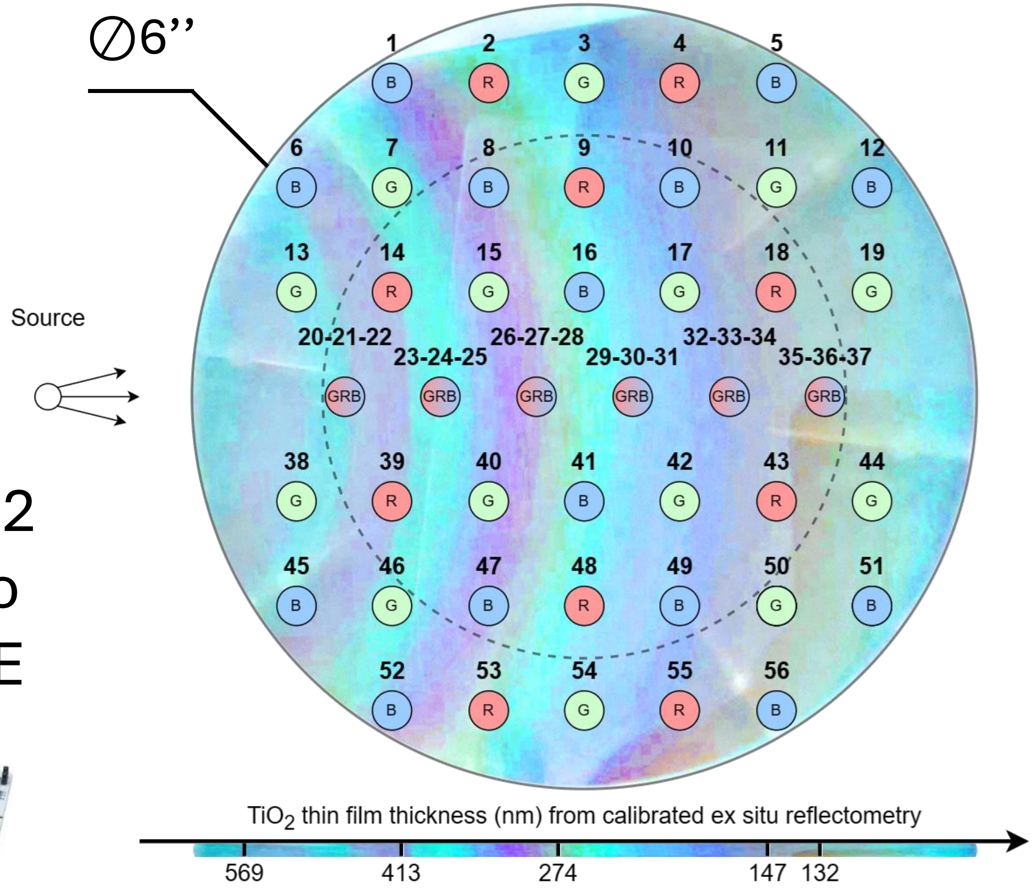
Macroscopic version

- No constraint on miniaturization
- Define setup to perform experiments
- Custom enclosure with:
  - Stage of sources (LEDs)
  - Substrate plate (up to 6” wafers)
  - Stage of sensors (photodiodes)



+ STM32 Nucleo L452RE

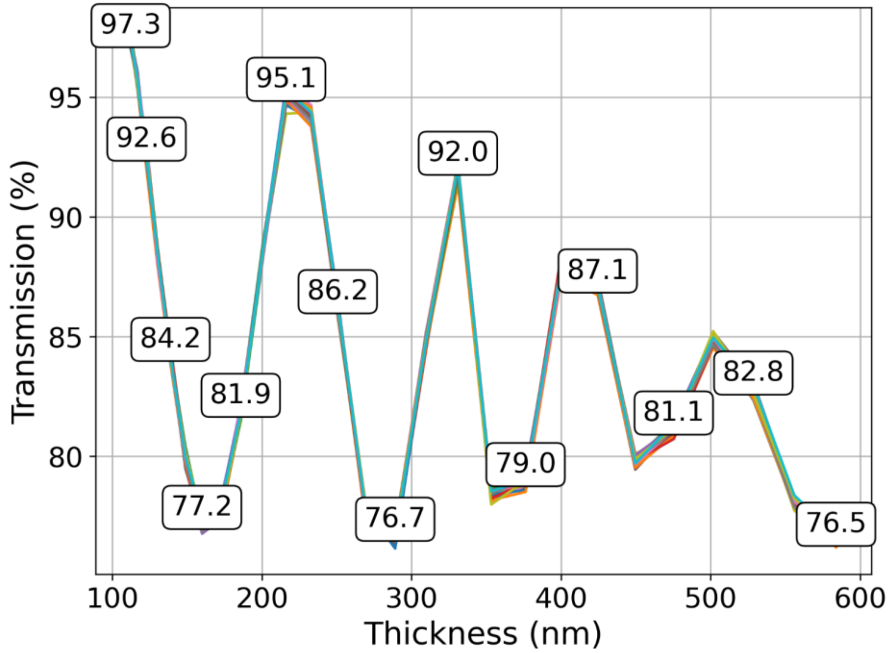
Top view of 150 mm transparent wafer with thin film layer showing interferential colors



56 challenges

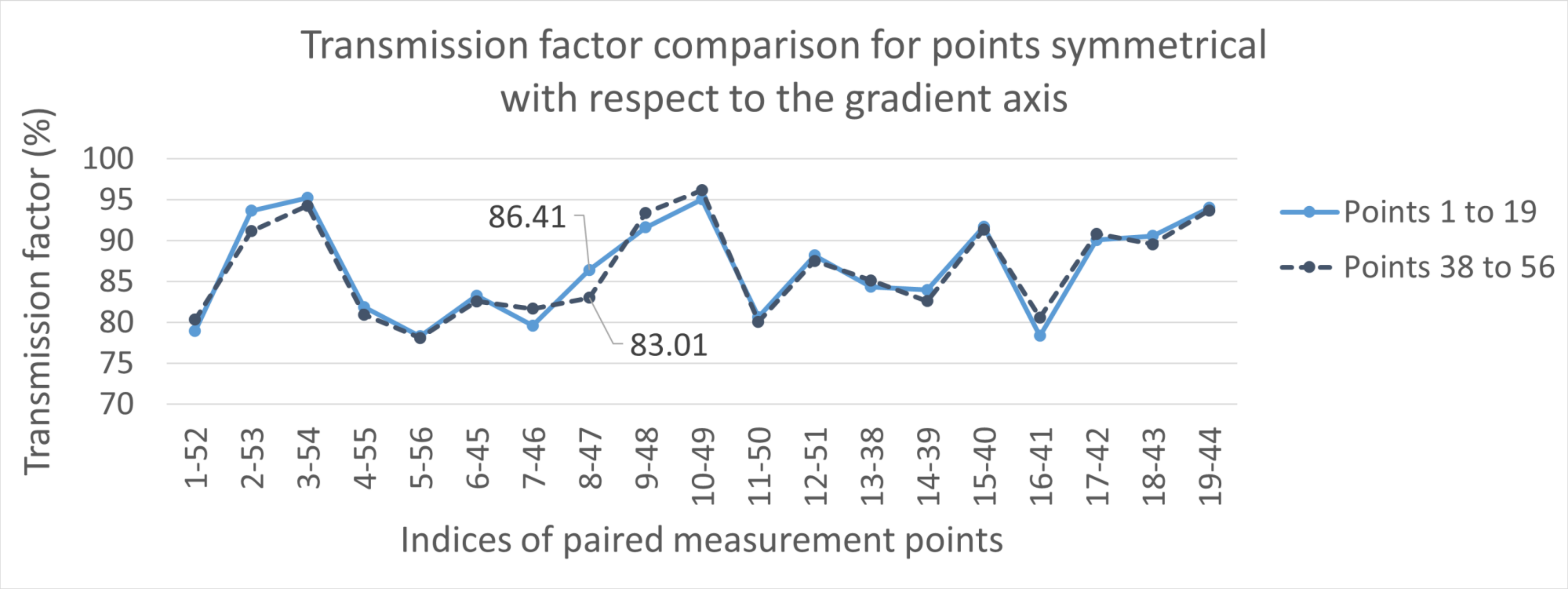
Thin film thickness impact

- Optical transmission variation (for a given diode wavelength) vs TiO_2 thin film thickness variation of about 34 nm steps
- 2,500 acquisitions grouped by block of 50
- Range between 76 % and 97 %
- Distinguishable oscillations, diminishing as thickness increases



Symmetry with the gradient axis

- Axes of symmetry of the thin film and the system aligned
- Relative deviation (≤ 4 %) lower than worst case on transmittance

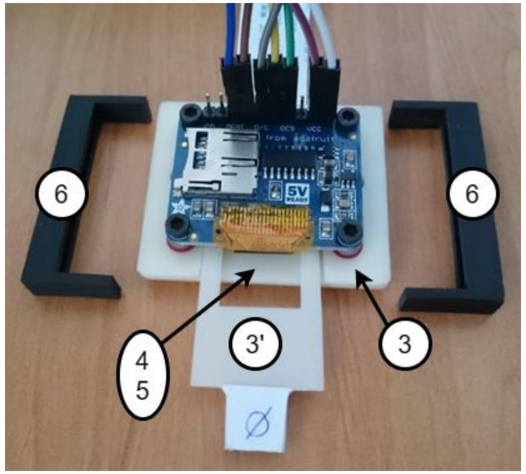


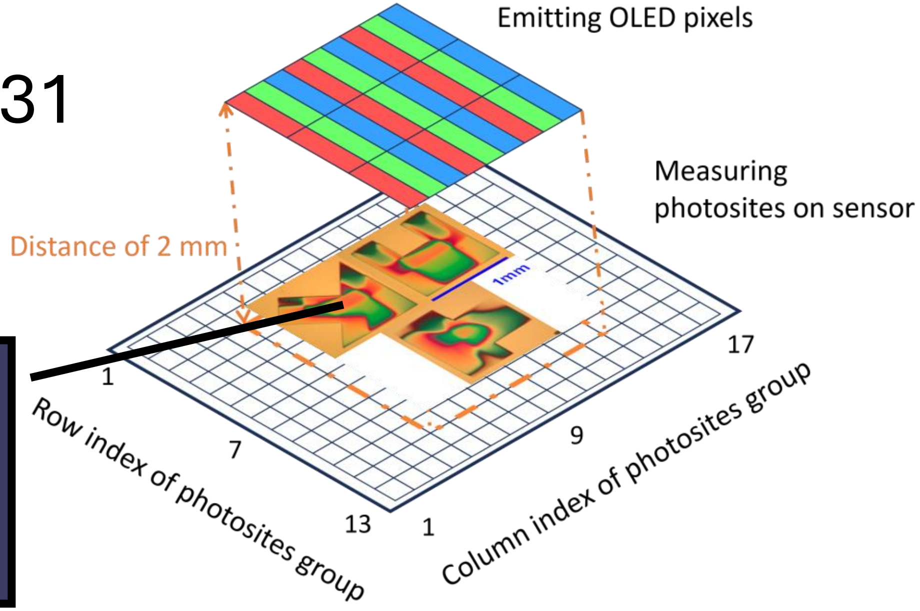
Notes on macroscopic version

- Limited by electronic components and basic design
  - Noise not properly filtered, but with temporal averaging
- Capacity of diversification mainly limited by low reliability
  - 56 points of measurement (N) with 1 wavelength (Z)
  - $L^{Z\times N} = \lfloor(100-74)/6.5\rfloor^{1\times 56} = 4^{56} = 2^{112}$
- Enclosure is custom built, but manual handling is detrimental to alignment
- Test limited to one (large and costly) system
- Not sufficient as MVP → Move to a compact version

Compact version

- Miniaturization and integration of PUFs and Twin PUFs
- Same concept but different HW & SW
- Sensor: Raspberry Pi Camera Module V2 (10-bit Sony IMX219)
- Display: 96x64 OLED display with SSD1331 driver (Adafruit 684)
- Introduces flicker phenomenon, Bayer filter and microlenses





Gradient (thickness and or composition) on µm scale

4. Results and Discussion

Experiments performed on the system

Preliminary experiments

Dark current
Range reduced by 6% & 0.02% Hot points

Flat field
Close & Distant sources

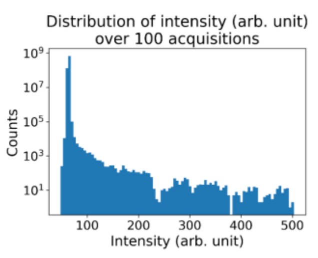
Bayer filter and **Micro-lenses**

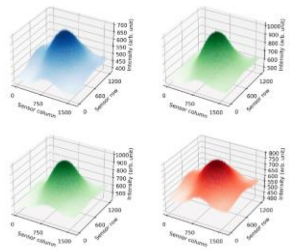
Calibration

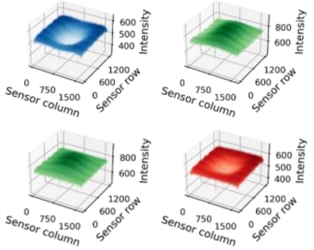
Intensity stability of OLED display

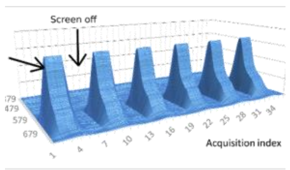
Temporal averaging effect on noise
20% → 3%

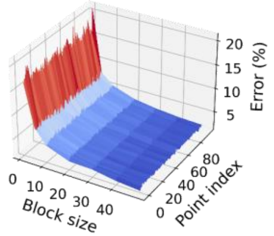
Spatial averaging Display & Sensor
15% → 10%
20% → 2%

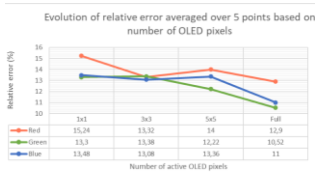












Range of parameters to create stimuli

- Method: Determine the minimal change in the challenge that has a greater impact than noise on response

- Approach 1: Distinguishing raw values according to pixel color

  → Limit sub-pixel command to 4-bits

- Approach 2: Distinguishing raw values according to angle between OLED pixel and group of photosites

  → 1 out of 3 columns on horizontal axis

  → 1 out of 6 rows on vertical axis

Theoretical capacity of diversification

- RGB command: $2^{4^3} = 4096$
- Angle pixel / photosites: $6\ columns \times 2\ rows$

→ $Z = 2^{4^3} \times 6 \times 2 = 3 \times 2^{14}$

- Sensor operating range: ~ 950 (10-bit depth minus dark current)
- Relative variation: ~ 0.02

→ $L = \frac{950}{950 \times 0.02} = 50$

- Pixel binning: 31×31

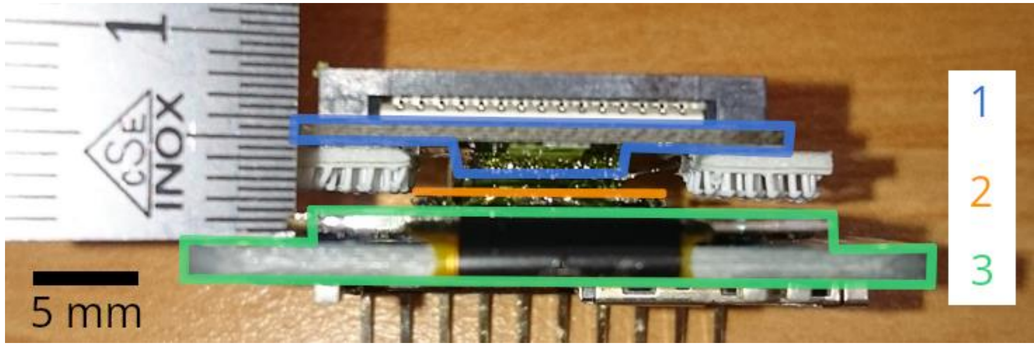
→ $N = 4 \times \lfloor 1640/31 \rfloor \times \lfloor 1232/31 \rfloor = 8112$

→ $L^{N \times Z} = 50^{8112 \times 3 \times 2^{14}} \approx \mathbf{2^{10^9}}$

(vs 2^{112} on macroscopic version)

Responses based on raw values

- 260 CRPs repeated x100 concatenated into strings (pixel position and RGB command, position of group of photosites)
- Consider standard statistical performance indicators (uniformity, uniqueness, reliability, intra- and inter-distances) for different parameters:
  - Encoding
  - Temporal averaging
  - Bit depth
  - Distribution centering
- Observe the influence of temperature



1 CMOS sensor
2 Homogeneous TiO_2 thin film
3 OLED display

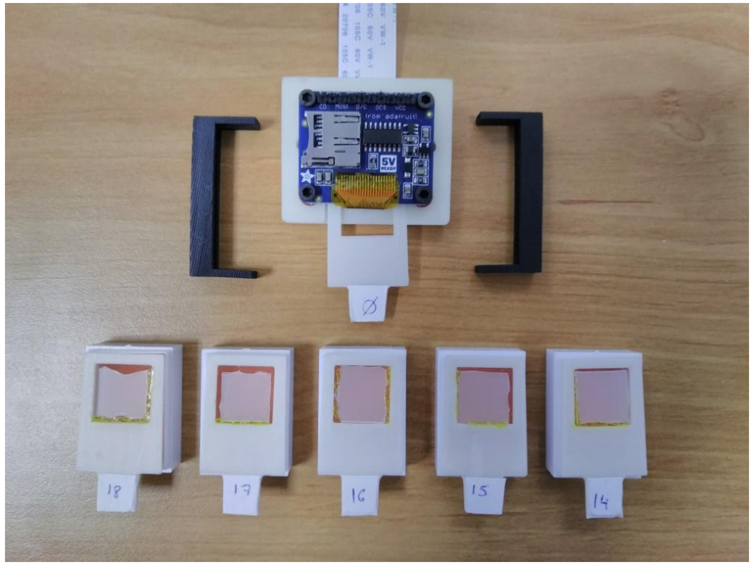
Responses based on transmittance

- Calibration without sample
- Enable successively OLED pixels
- Save groups of photosites (x10)
- Median of all configurations for binarization

→ Low uniqueness:

  - Few percents
  - Even with smaller groups
  - Or $LiNbO_3$ thin film

→ Invalid binarization step



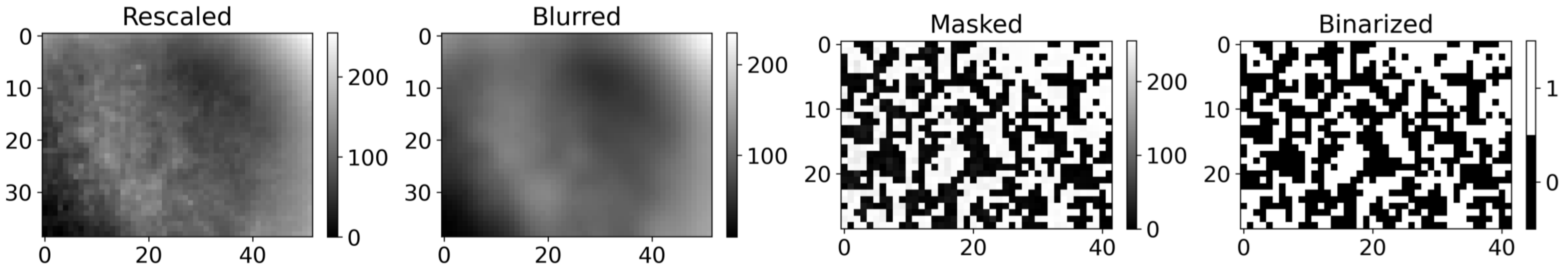
x5 TiO_2 on fused silica samples (465 nm)

Responses based on local variations

- Introduce processing to manage acquisitions and isolate thin film contribution → Transmittance with **unsharp mask** and local variation, and matching sub-pixel with color filter

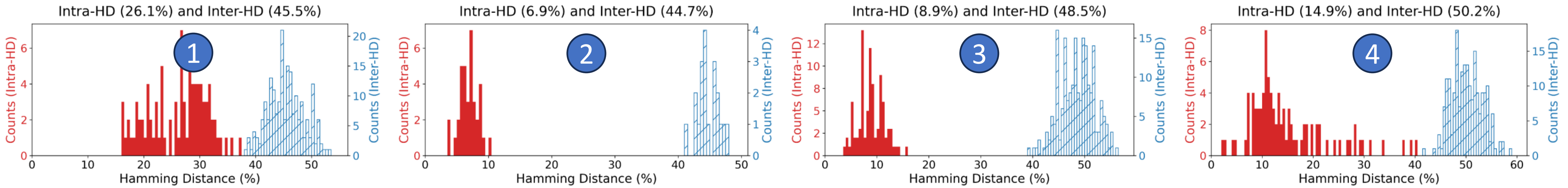
Scale → Blur filter → Difference (mask) → Cropping → Median → Binarization

Kernel 31x31 - CRP 0 - Green Sub-pixel - Row screen 6 - Column screen 1 - Green (TR) Bayer filter - Acq 0 - $LiNbO_3$



Responses based on local variations

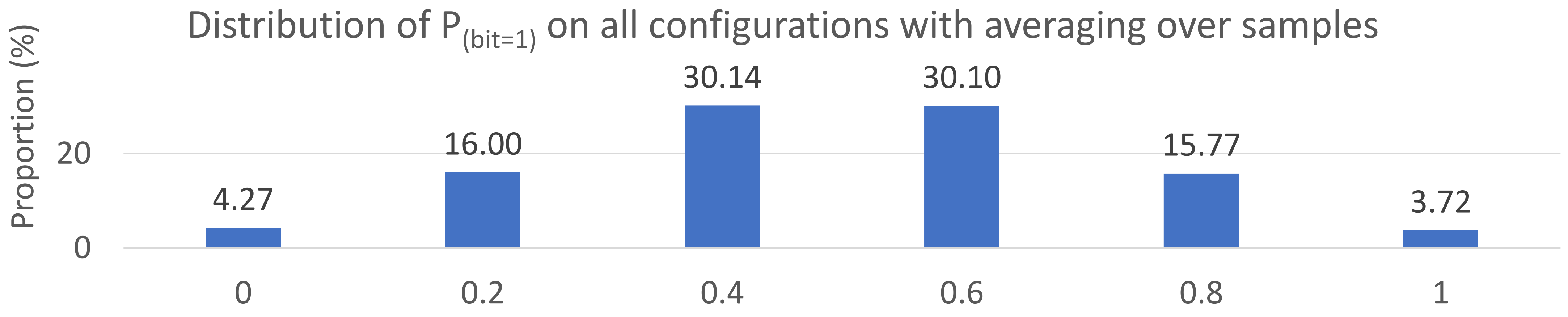
	Temporal stability (%)	Reliability (%)	Uniformity (%)	Uniqueness (%)	Intra-HD (%)	Inter-HD (%)	Gap
Ideal values	0	100	50	50	0	50	50.0
TiO_2, 465 nm, Fused silica (1)	0.42	73.9	46.5	45.5	26.1	45.5	19.4
$LiNbO_3$, 345 nm, Sapphire (2)	0.33	93.1	49.3	44.7	6.9	44.7	37.8
TiO_2, 312 nm, Rough sapphire (3)	0.44	91.1	51.4	48.5	8.9	48.5	**39.6**
Rough sapphire substrate (4)	0.69	85.1	48.8	50.2	14.9	50.2	35.3
TiO_2, 456-484 nm, Rough sapphire	0.43	85.8	48.4	46.4	14.2	46.4	32.2
TiO_2, 400-428 nm, Rough sapphire	0.57	89.6	48.9	47.9	10.4	47.9	37.5
TiO_2, 316-344 nm, Rough sapphire	0.44	89.1	49.3	49.6	10.9	49.6	38.7



Statistical analyses

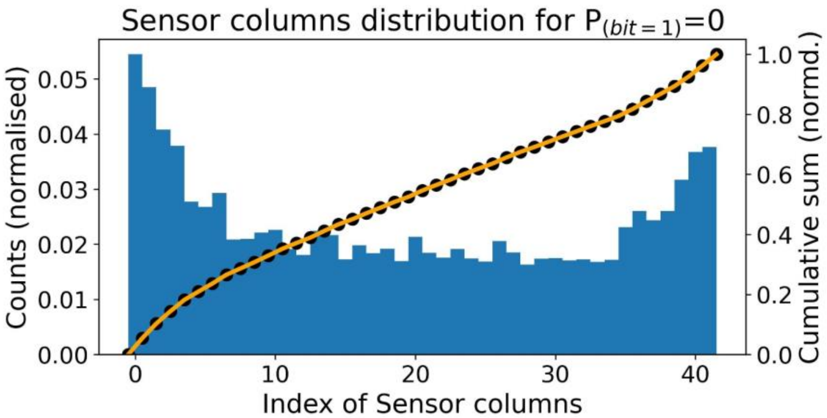
- Based on responses from 5 homogeneous TiO_2 on rough sapphire samples
- 1,875,720 bits in the data set
  - Bit probability along samples axis to check common responses

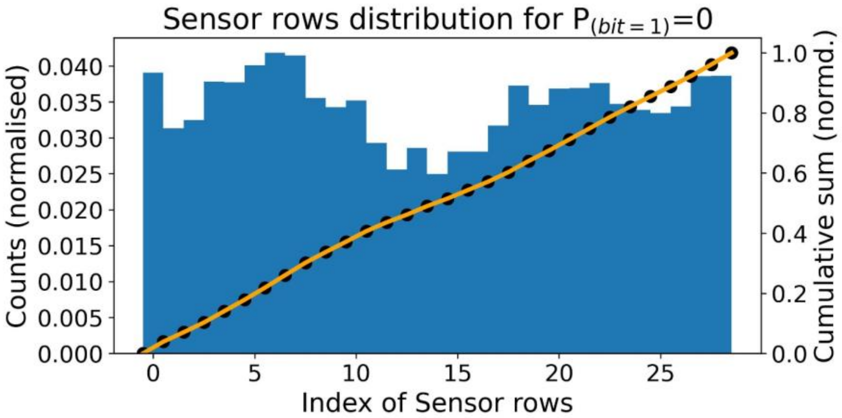
  → 4.27 + 3.72 = **7.99 %** of the responses are **common to all samples**

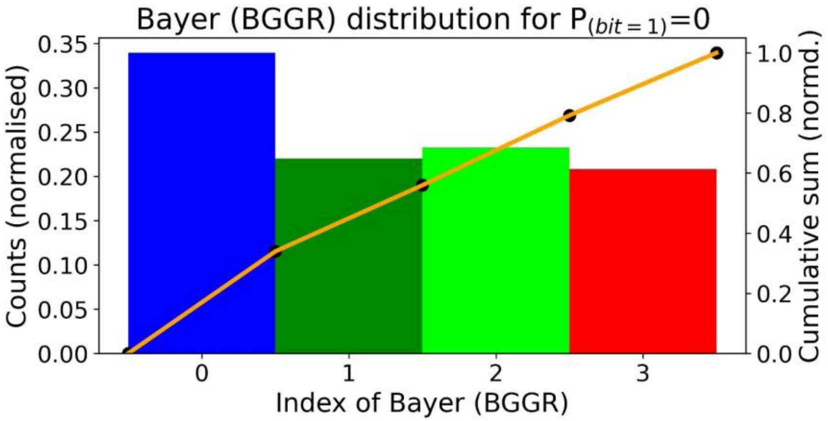


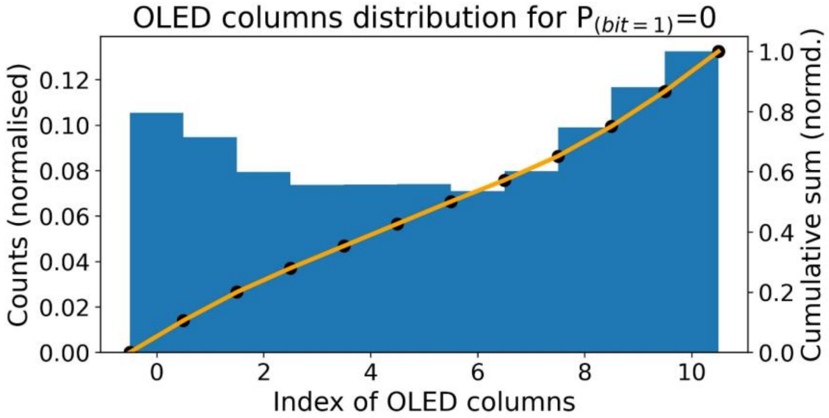
Statistical analyses

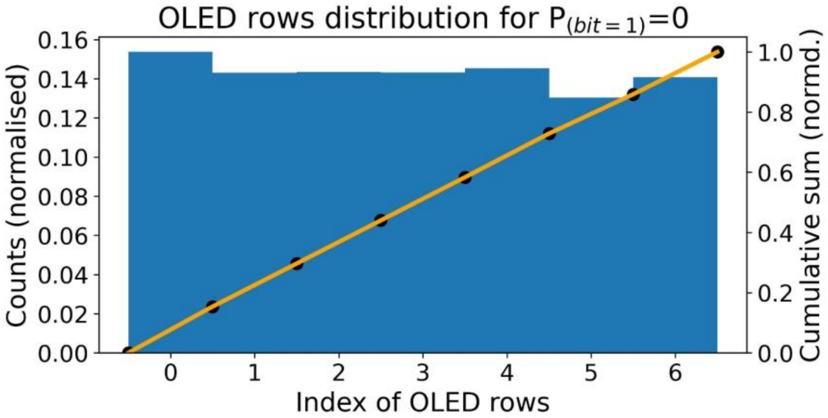
- Identify configurations potentially biasing those responses
  - → OLED pixel and CMOS sensor photosites combination for $P_{(bit=1)} = 0$





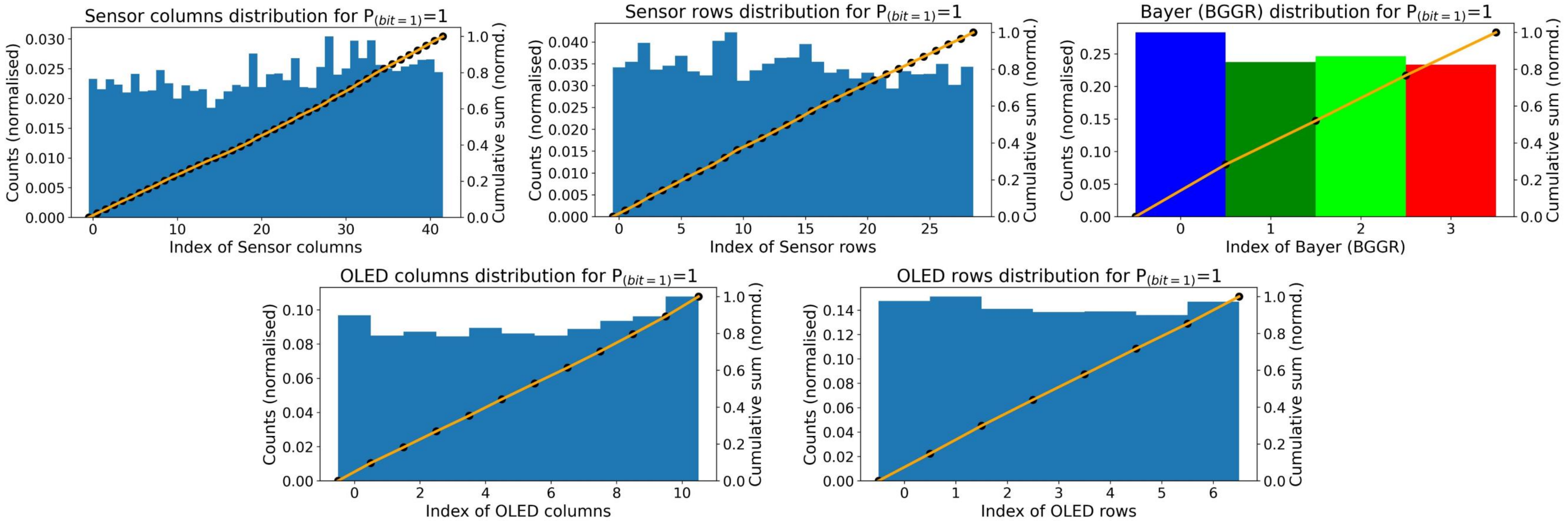




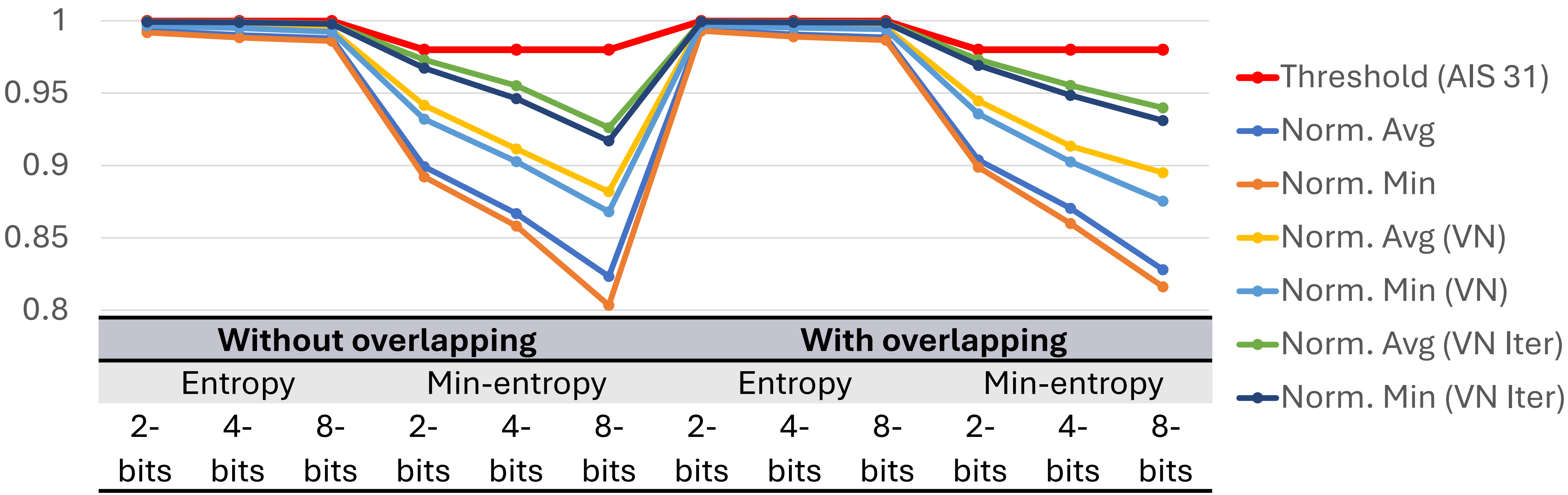


Statistical analyses

- Identify configurations potentially biasing those responses
  - → OLED pixel and CMOS sensor photosites combination for $P_{(bit=1)} = 1$



Impact of debiasing methods



- Average entropy without overlapping for 2-bits patterns:
  - With classic Von Neumann method: 0.9976
  - With iterative Von Neumann method: 0.9995

5. Conclusion and Outlook

Current limitations and avenue for improvement

Conclusion

- Significant theoretical capacity of diversification
  - Multifunctional patterned oxide thin films (like 10^{15} bits/mm^2)
  - Twin PUF concept
- Complex to miniaturize and integrate
  - Too limited macroscopic version
  - Unoptimized compact version
- Different methods addressed to define responses
  - Main concern: isolate effect of thin film
  - Limit the capacity of diversification
- Improvements needed to meet current standards

Outlook

- Detailed model and resilience
- Monolithic integration
- Efficient calibration method
- Alternative physical properties to solve main bottlenecks
  - Component cost, delay, energy consumption, and footprint
- Compatibility with security architecture

Contact information

Thank you for your attention

- Company website: https://www.3d-oxides.com/
- Chief Technical Officer: Giacomo Benvenuti giacomo.benvenuti [at] 3d-oxides.com
- benjamin.malthiery [at] 3d-oxides.com