Institut des Nanotechnologies de Lyon UMR 5270

Recent Advances in Photonic Physical Unclonable Functions

Fabio Pavanello

20/05/2021

Journée thématique : Emerging technologies in security applications

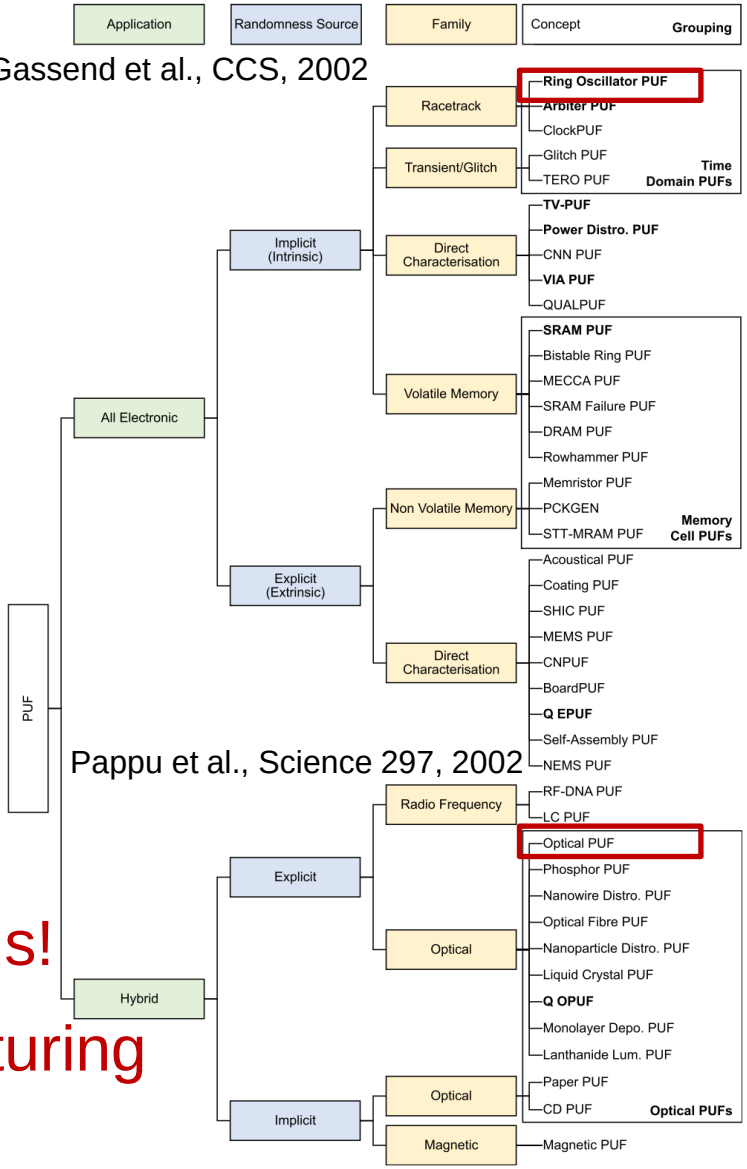
Outline

- Introduction to PUFs
- Electronic PUFs and current limitations
- The photonics advantage
- Photonic PUFs: challenges and opportunities
- Conclusions and perspectives

Intro to PUFs: Basic properties and landscape

- Physical uniqueness
- Physical unclonability
- Digital unpredictability
- Reliability
- Reasonable costs and efficiency

Gassend et al., CCS, 2002



Pappu et al., Science 297, 2002

Electronic PUFs dominate industry focus!

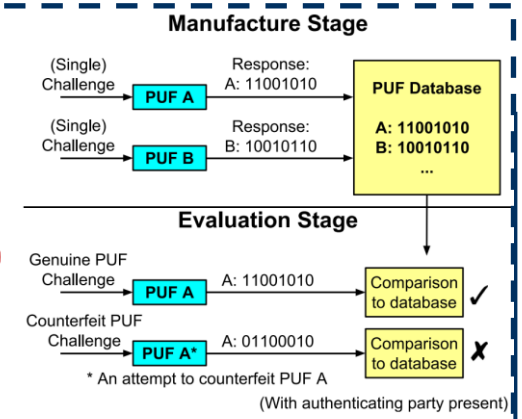
Recent advances in modeling/manufacturing may be changing this…

McGrath et al., Appl. Phys. Rev. 6, 2019

PUFs: Applications

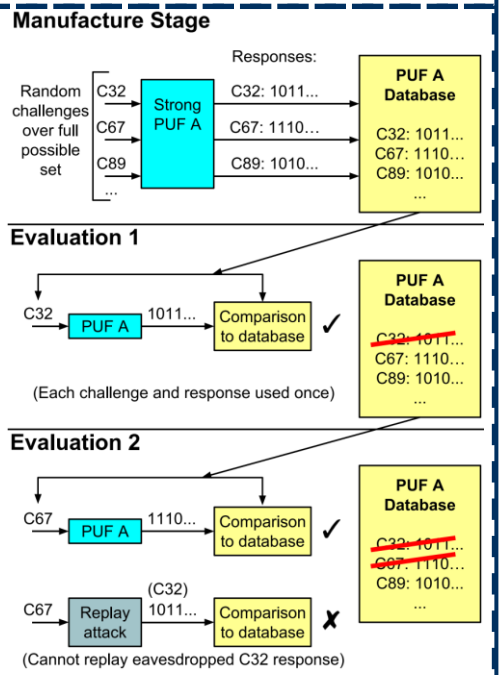
- Hardware integrity
- Secret key generators

Weak PUFs
(small set of CRPs)



- Secure authentication
- Secure key exchanges
- Bit committment & oblivious transfer

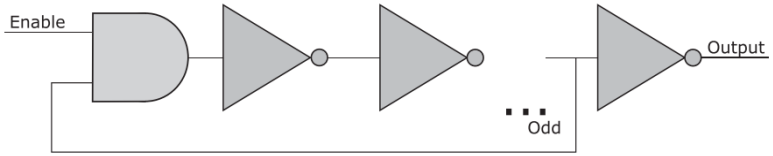
Strong PUFs
(large/exponentially scaling set of CRPs)



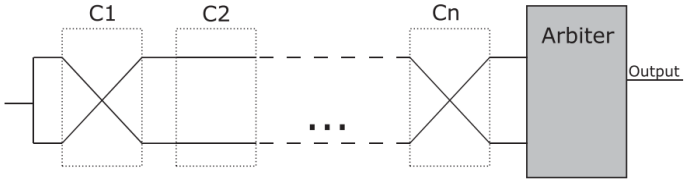
McGrath et al., Appl. Phys. Rev. 6, 2019

Electronic PUFs: Ring Oscillators and Arbiter PUFs

- Ring Oscillator PUFs
  - Based on fabrication tolerances affecting nominal gate delays
  - Odd number of inverters in a feedback loop
  - Challenge is sent through a multiplexer to multiple oscillator chains
  - Response based on a comparison of oscillation frequencies



- Arbiter PUFs
  - Based on fabrication tolerances affecting nominal gate delays
  - Signals from cascaded multiplexer stages are compared by arbiter stage which outputs a response bit (based on signal arrival timings)
  - Challenge is encoded according to the position of the stages
  - XOR functions can be added to introduce non-linearity



McGrath et al., Appl. Phys. Rev. 6, 2019

Electronic PUFs: possible attacks

- Side-channel passive & active attacks (see Bossuet, ECCTD2020 and Delvaux & Verbauwhede, CSI 61, 2014):
  - RF radiation from the circuits
  - Photonic emission by the back-side of the chip
  - Fault injection (forcing more instable CRPs)

- ML attacks (see Regazzoni et al., ICCAD2020)
  - Demonstrated effective on several types of PUFs (Arbiter, RO…)
  - Successful due to the rather simple scrambling mechanisms of signals in electronics implementations
  - ML attacks coupled with side-channel information demonstrated effective on XOR Arbiter PUFs

Need for solutions that are at the same time: low-cost, compact, energy-efficient and robust to attacks!

The photonics advantage: physical considerations

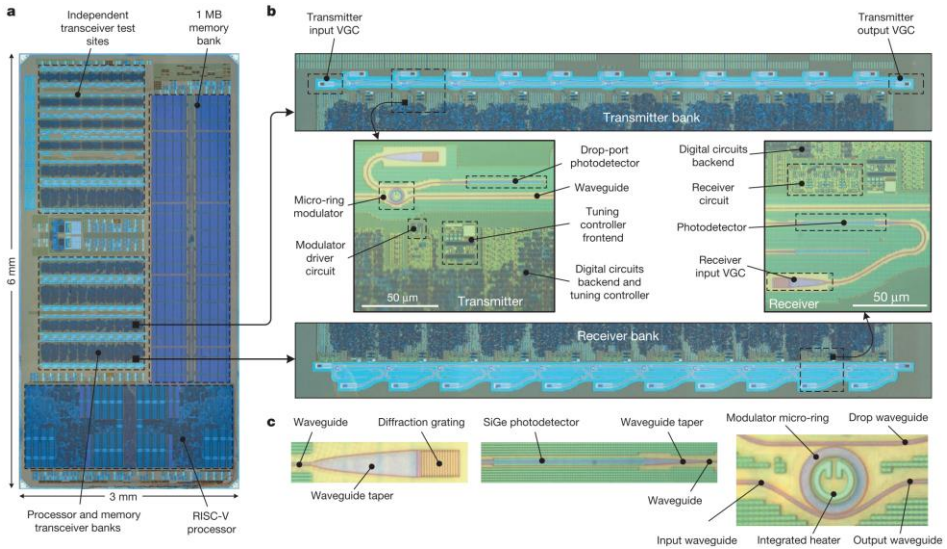
- Photonics allows to:
  - leverage several degrees of freedom: intensity, phase, polarization, multiple resonant and spatial modes
  - achieve compact footprints thanks to the rich underling physics
  - implement non-linearities in a multitude of ways: square law at photodetection, free-carrier dispersion/absorption, Kerr effect…
  - transfer signals in an analog way thus providing a much richer exploitation of the signal dynamic range
  - avoid radiation leakage during signal propagation (for integrated photonics circuits)

The photonics advantage: integration

- CMOS compatible & « zero change » platforms allow to:
  - reduce fabrication costs and prototyping time (open access system)
  - provide a simpler route to integration with ICs and testing
  - achieve high yield / reliability of performance

Foundry	Platform	Technology	Access	Waveguide Layer Thickness (nm)	Wafer Size (inch)
		RAPID PROTOTYPING SERVICES			
AMO	thin SOI SiN	e-beam	Direct	220, 340	6
Applied Nano Tool	thin SOI	e-beam	Direct	220, 300	6
CNM/VLC	SiN	e-beam	Direct	300	4
Cornerstone	thin SOI	248 nm	Direct	220, 340, 500	8
LIGENTEC	SiN	-	Direct	up to 2500	4/6
		CMOS PILOT LINES & RESEARCH INSTITUTES			
AIM (SUNY)	thin SOI	-	MOSIS	-	12
	SiN	-		-	12
CEA-LETI	thin SOI	193 nm	CMP	310	8
	Ge/SiGe			up to 3000	8
IHP	SiGe BiCMOS	248 nm	Europractice	220	8
IMEC	thin SOI	193 nm	Europractice	220	8
	SiN		Direct		8
IMECAS	thin SOI	-	SPP	220	8
INPHOTEC	thin SOI	e-beam	Direct	220	6/8
Sandia Lab	thin SOI	-	Direct	240	
VTT	thick SOI	UV	Direct	3000	6
		INDUSTRIAL FABS			
AMF(former IME)	thin SOI	248/193 nm	Direct†	220, 340	8
	SiN			-	8
	SiN-on-SOI			-	8
CompoundTek	thin SOI	193 nm immersion	Direct	-	-
Global Foundry/IBM	thin SOI	193 nm immersion / 248 nm	MOSIS, Direct, TAPO	sub-100 nm	8/12
SilTerra	thin SOI	-	Direct	-	8
SMIC	Thin SOI	-	Direct	340	8
ST Micro§	thin SOI	193 nm	Direct	310	12
TowerJazz	thin SOI	193 nm	Direct	-	8
TSMC	thin SOI	-	-	-	12
LioniX	SiN	UV	Direct	flexible	-

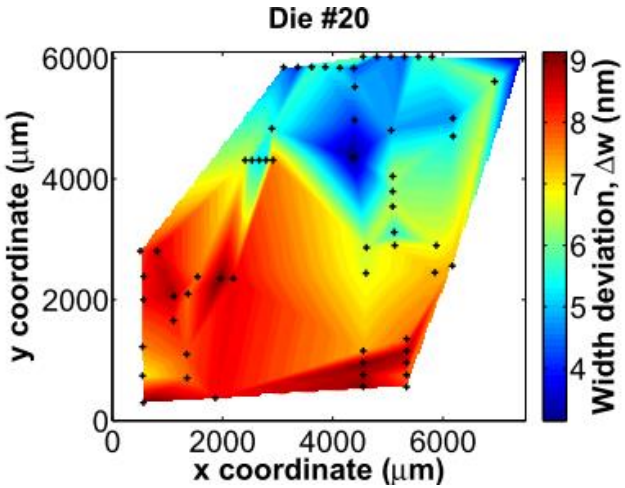
Rahim et al., Proc. IEEE 106, 2018

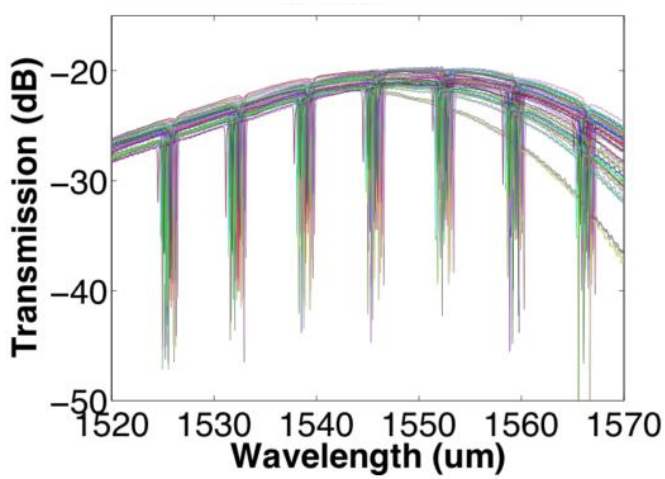


Sun et al., Nature 528, 2015

First processor to memory optical link → large yield of photonics and tight co-integration of electronics

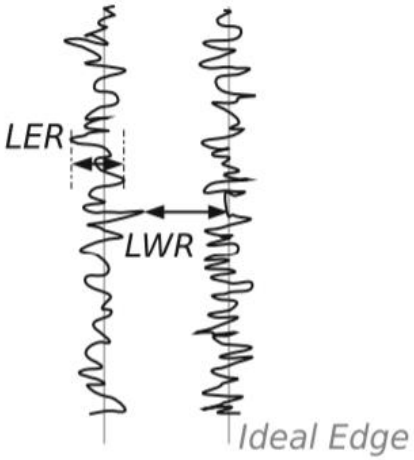
The photonics advantage: fabrication tolerances

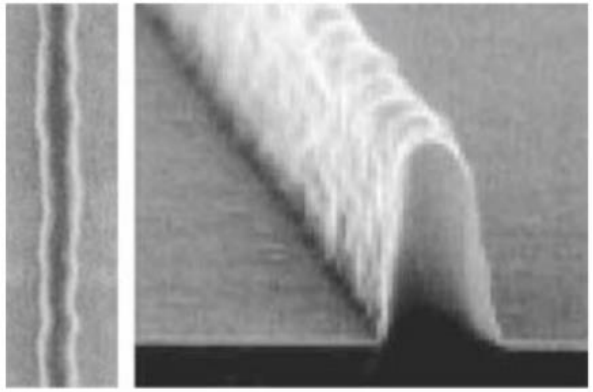




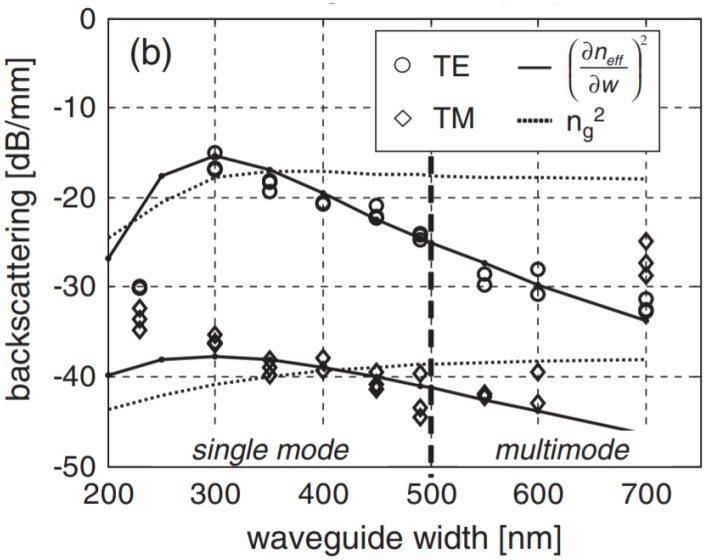
Lu et al., Opt. Exp. 25 (9), 2017

- Layer thickness
- Device widths
- Delay lengths
- Doping profiles
- Roughness





Maricau and Gielen, Analog IC Reliability in Nanometer CMOS, Springer, 2013



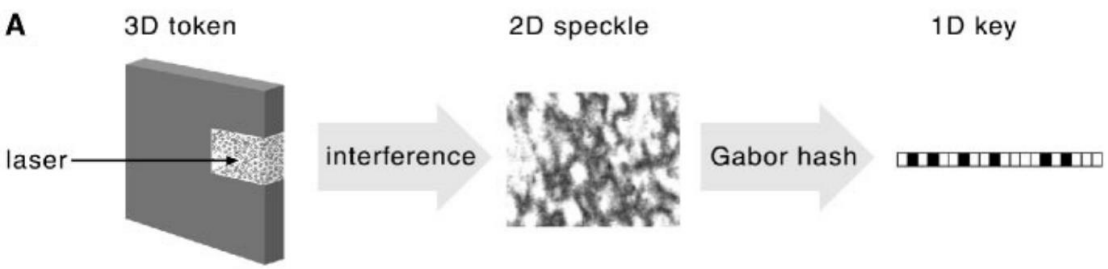
Morichetti et al., Phys. Rev. Lett. 104, 2010

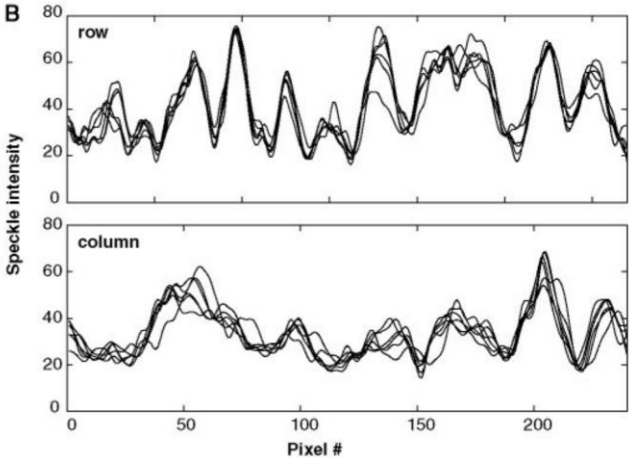
Photonic PUFs: the origins

REPORTS

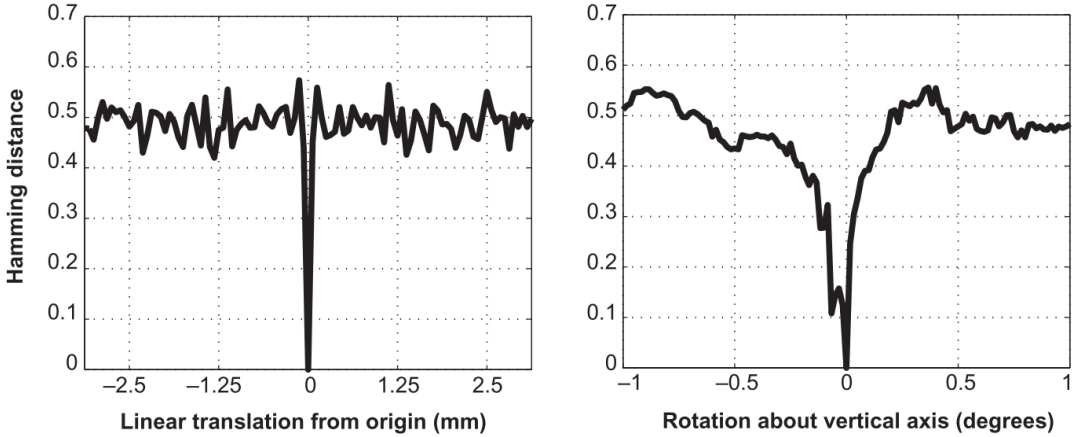
Physical One-Way Functions

Ravikanth Pappu,*† Ben Recht, Jason Taylor, Neil Gershenfeld





- Bulk optics
- Diffraction-based
- Costly
- Low robustness
- High testing cost



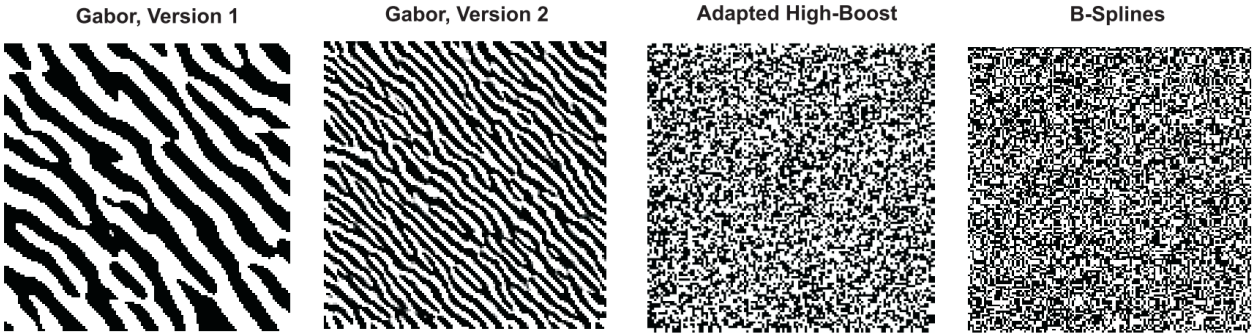
Pappu et al., Science 297 (5589), 2002

Photonic PUFs: ML-resilience of the original approach

- ML attacks @ TU Munich using 100k raw speckle images <u>unsuccessful</u> – e.g. SVM with lin. kernels → err rates ~ 50%

- ML feature vectors <u>too large to be handled</u> (order of 10^{11} volume units). 128-bit arbiter: feature vector has 129 entries

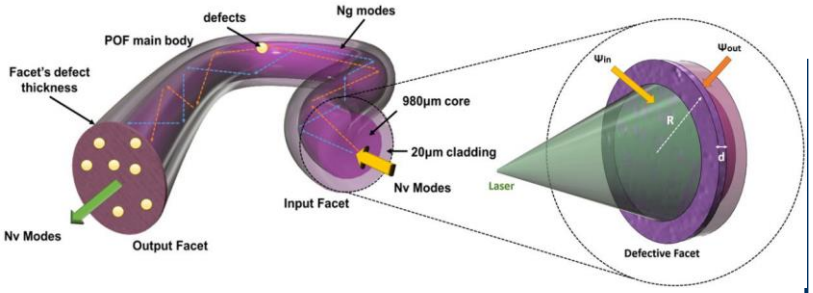
- More advanced mathematical transformations e.g. wavelet transformations allow to remove pattern regularities (4x more independent bits)



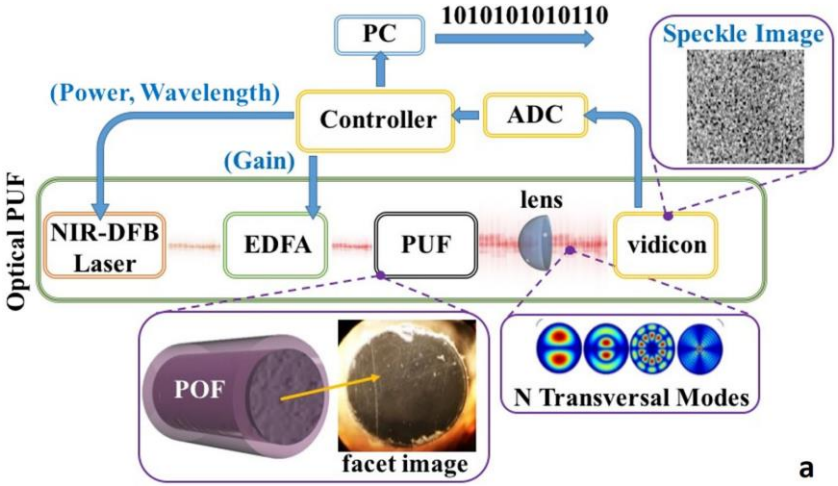
Ruhrmair et al., IACR Cryptology, 2013

Photonic PUFs: linear approaches

- Polymeric optical waveguide with imperfect facets
- Number of modes excited ~ 10^6
- Complex mode mixing based on the scattering matrix of the fiber
- Spatial input light modulation to encode challenges



Mesaritakis et al., Sci. Rep. 8, 2018

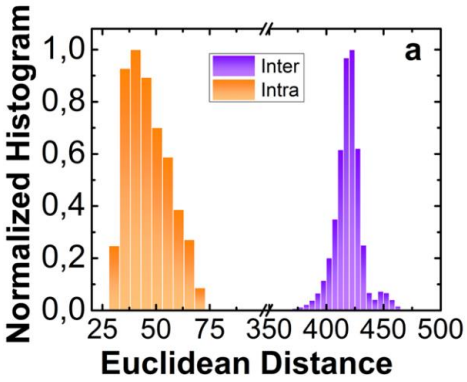


Although scattering is linear, the read-out presents a square law → optical delay differences contribute in a non-linear coherent way

CNNs can so far only model very small diffuser areas: Maxwell equations are complex to solve… see Li et al. Optica 5, 2018

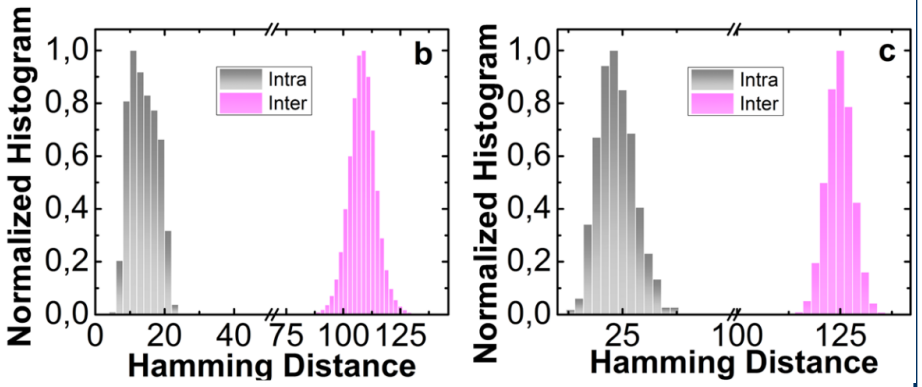
Photonic PUFs: linear approaches

- Proven robustness from raw images: inter (copies) and intra (same PUF) distributions do not overlap!



- Strong robustness to noise: transformation type, random (b) or Gabor (c) binary hashing does affects Hamming distance

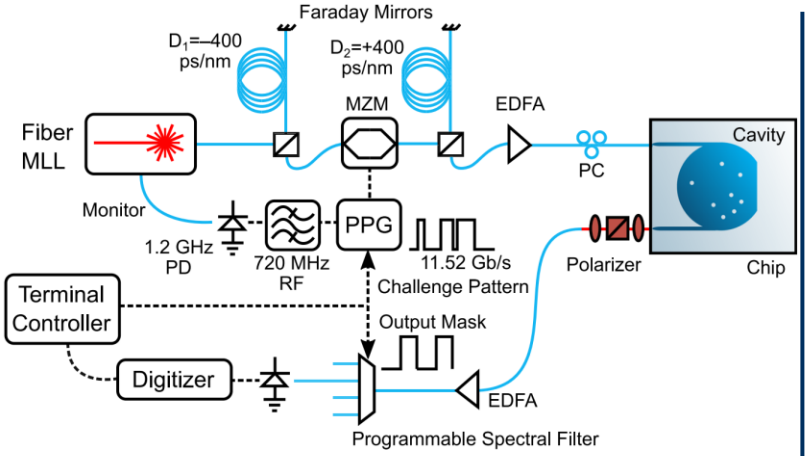
  (255-bit word)

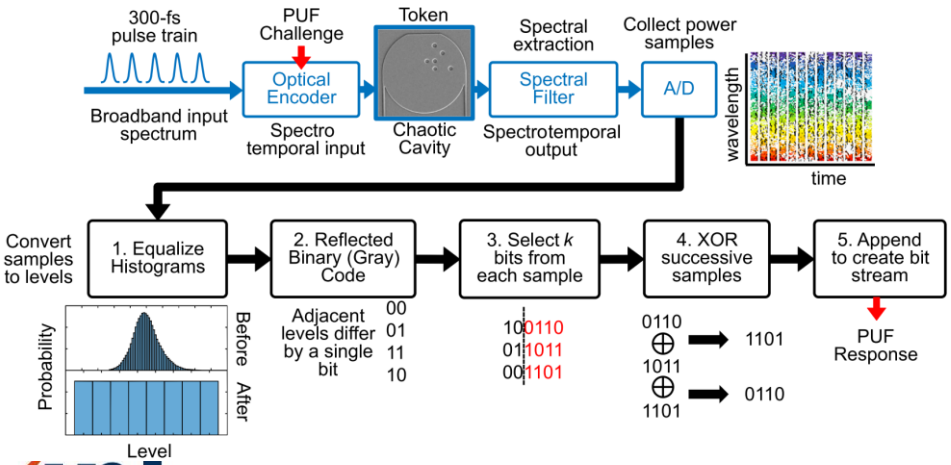


Mesaritakis et al., Sci. Rep. 8, 2018

Photonic PUFs: non-linear approaches

- Si chaotic cavity → complex mixing of spectrotemporal features
- MLL laser provides a reliable syncronized input signal which triggers non-linear phenomena
- Challenge is encoded onto the stretched pulse before being compressed back





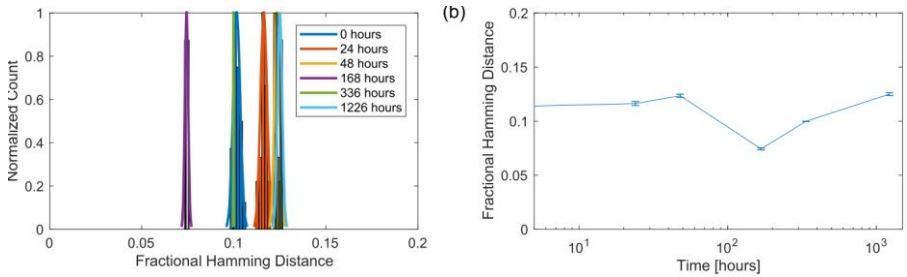
Post-processing of the samples to enhance robustness!

XOR function used for higher binary complexity

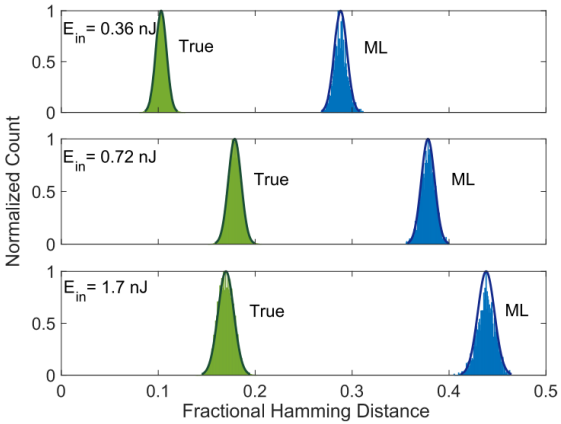
Bosworth et al., APL Photonics. 5, 2020

Photonic PUFs: non-linear approaches

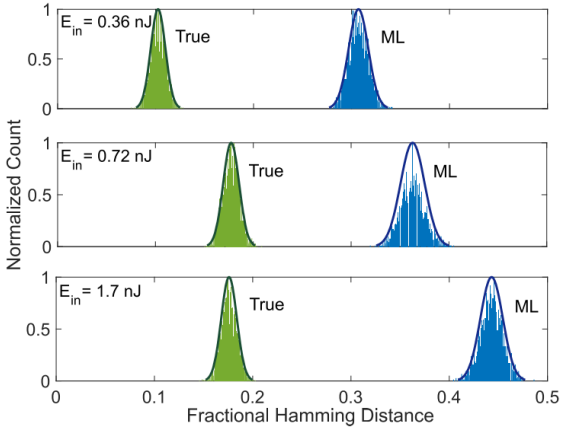
- High stability of the PUF responses over time



- ML attacks on output digital responses:
  - 100k CRPs for training (before plateau)
  - 9.9kbit keys
  - 128bit challenges/DNN input nodes
  - <u>Non-linearity increases unpredictability</u>



- ML attacks w side channel information:
  - Raw analog power values before digitizer
  - Bit extraction on the DNN predicted powers
  - As before good separation btw genuine and ML-predicted responses



FAR and FRR cross at 10^{-22}

Bosworth et al., APL Photonics. 5, 2020

Conclusions

- Current electronic PUF solutions present limitations in terms of robustness to ML and side channel attacks, reliability (e.g. aging), footprint and power consumption (ECCs)

- Photonic solutions may provide a viable path to solve these issues by leveraging the complex physics behind their operation and their CMOS-compatibility

- Existing photonic PUFs (even the original version) have shown a large ML-resilience and noise robustness

- Photonic PUF demonstrators have already been fabricated in CMOS-compatible platforms

Perspectives

- Need to scale down testing methods/apparatus and to implement all the main components on chip for reliability and cost

- Development of robust electronic driving interfaces adapted to photonic PUFs

- Investigation of trade-offs between complexity and ML-resilience

- Demonstration of photonic PUF prototypes at high TRL (>6)

Closing announcements

- JCJC ANR project PHASEPUF: Photonic Augmented SEcurity via Physical Unclonable Functions (AAPG2020 - CES39) started this April!
  - Objective: to develop novel robust and CMOS-compatible photonic PUFs
  - Looking for a talented PhD student to join the project

PHASEPUF

AGENCE NATIONALE DE LA RECHERCHE ANR

- ETS2021: special session on Recent Advances in Photonic Physical Unclonable Functions
  - More info: https://ets2021.eu/
  - Session time: 26 May @ 2pm