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

Electronic PUFs dominate industry focus!
Recent advances in modeling/manufacturing may be changing this…

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

http://inl.cnrs.fr
PUFs: Applications

- Hardware integrity
- Secret key generators

Weak PUFs
(small set of CRPs)

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

Strong PUFs
(large/exponentially scaling set of CRPs)
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
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

Rahim et al., Proc. IEEE 106, 2018

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

Sun et al., Nature 528, 2015
The photonics advantage: fabrication tolerances

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

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

Photonic PUFs: the origins

- 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 unsuccessful – e.g. SVM with lin. kernels → err rates ~ 50%

• ML feature vectors too large to be handled (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 $\sim 10^6$
- Complex mode mixing based on the scattering matrix of the fiber
- Spatial input light modulation to encode challenges

Although scattering is linear, the read-out presents a square law $\rightarrow$ 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)
Photonic PUFs: non-linear approaches

- Si chaotic cavity → complex mixing of spectrotemporal features
- MLL laser provides a reliable synchronized 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
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
    - Non-linearity increases unpredictability

- 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 $10^{-22}$
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

• ETS2021: special session on Recent Advances in Photonic Physical Unclonable Functions
  – Session time: 26 May @ 2pm