Photonic Physical Unclonable Function Based on Symmetric Microring Resonator Arrays

Paul Jimenez,[1,*] Raphael Cardoso,[1] Maurício Gomes de Queiroz,[1] Mohab Abdalla,[1,2] Clément Zrounba,[1] Xavier Letartre,[1] Cédric Marchand,[1] Ulrich Rührmair,[3] Fabio Pavanello,[1]

[1] *Univ. Lyon - CNRS, École Centrale de Lyon, INSA Lyon, Université Claude Bernard Lyon 1, CPE Lyon - INL, UMR5270 - Écully, F-69134, France*
[2] *School of Engineering, RMIT University, Melbourne, VIC 3000, Australia,*
[3] *ECE Department, University of Connecticut, Storrs 06269, CT, USA*

[*] *paul.jimenez@ec-lyon.fr*

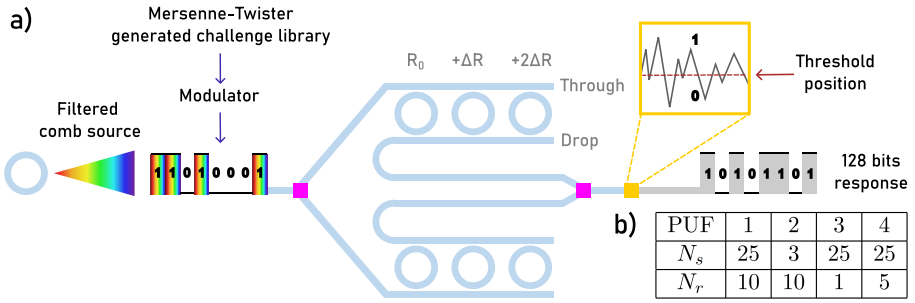
Abstract: We propose a novel architecture for a photonic Physical Unclonable Function (PUF) based on microring arrays. We demonstrate its uniqueness, verify its random behavior on standard benchmarks, and investigate the impact of the digitization threshold.

1. Introduction

Security layers relying on the digital storage of secret keys in memory are prone to various pitfalls, namely specific memory portions can be accessed in a malicious manner, therefore potentially exposing sensitive data. Security primitives based on PUFs do not rely on the digital permanent storage in memory of sensitive data and have been indicated as one of the most suitable hardware-based solutions [1]. The security properties of PUFs rely on complex and uncontrolable features appearing during the manufacturing process making them unique, unclonable, and with unpredictable behavior. A PUF establishes a unique correspondence between inputs (challenges) and outputs (responses), thereby enabling the creation of a database of challenge-response pairs (CRPs). Electronic PUFs present various limitations due to the low number of physical quantities for encoding and manipulating information signals [1]. On the contrary, photonic approaches [2, 3] allow access to a large number of physical quantities and degrees of freedom. This richness can be leveraged to encode information and achieve a more complex manipulation of the optical signals, strongly affected by fabrication variations [1].

2. Architecture description

Here, we propose a novel high-speed photonic PUF architecture. It is based on symmetrical arrays of N_r silicon microring resonators and is presented in Fig. 1 (a). The first ring of each line has an initial radius $R_0 = 10$ µm and we add extra $\Delta R = 10$ nm on each consecutive ring radius. Challenges are generated using the Mersenne-Twister algorithm. A filtered frequency comb with N_s coherent spectral lines around $\nu_0 = 194.7$ THz separated by $d\nu = 125$ GHz is considered. Spectral lines are multiplexed and fed to a Mach-Zehnder modulator (MZM) which encodes the challenges onto the optical signal. A fast photodiode connected to a real-time sampling oscilloscope (25 Gb/s) is used to acquire the responses. As indicated in Fig. 1 (a), a threshold is set at a given value to perform the analog-to-digital conversion, effectively becoming a parameter as well.



b)

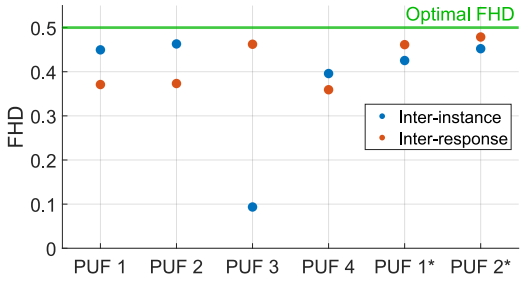
PUF	1	2	3	4
N_s	25	3	25	25
N_r	10	10	1	5

Fig. 1. a) Integrated photonic PUF architecture based on $N_r = 3$ silicon microring resonator arrays. Splitters are represented by pink squares, the photodetector by a yellow square. b) Number of rings and spectral lines considered for each PUF design.

3. Results and discussion

A mapping of fabrication variations on Silicon-on-Insulator (SOI) platform [4] has been used to emulate multiple realizations of PUF instances. After a preliminary convergence study, we first simulated 150 different instances of each design in Fig. 1 (b) using Lumerical INTERCONNECT™. To evaluate the randomness of each response we use six NIST statistical tests applicable to short bit sequences [5]. For the uniqueness, we compute the fractional hamming distance (FHD) [2] between instances (inter-instance FHD) and between the responses of a given instance (inter-response FHD). The targeted value is FHD = 0.5 which corresponds to the FHD between two uniform random processes [2]. In addition, we want the responses not to be biased, therefore, the threshold position is optimized for each challenge but not for each instance, i.e, for a given challenge the concatenation of all instances' responses is not biased. However, some individual responses to certain instances can be biased due to specific fabrication variations. This approach has been studied to have a threshold not depending on the instance. This is useful if we want to use the PUF with a fixed small library for all instances.

a)



b)

Test \ PUF	1	2	3	4	1*	2*
Frequency	3	3	27	5	100	100
Frequency (block)	7	6	58	10	100	100
Run	3	2	24	5	46	32
Run (block)	9	4	35	7	73	44
Cumulative Sums	71	71	35	72	100	100
Approx. Entropy	1	2	46	3	7	6

Fig. 2. a) Average inter-instance and average inter-response FHD of the different designs. b) Percentage of instances passing the considered NIST tests for each PUF design presented in Fig. 1 (b).

As presented on Fig. 2 (a) PUF 1 and PUF 2 obtain the best FHDs. However, as shown Fig. 2 (b), few instances of PUFs 1-4 passed the NIST tests, mostly because many were considered as biased, with the exception of PUF 3 achieving good scores in its NIST tests, but with a low inter-instance FHD. This is due to the fact that PUF 3 with its single ring retains the quality of randomness and bias of the challenge, as if it were partly "transparent" on these criteria and therefore does not have enough effect to have a high FHD between instances. This is an example where the quality of the challenge can artificially improve the results of statistical tests and why it is important to rely on more than one metric. Therefore, optimizing a threshold for each response but not for each instance can only be used if we can deal with the bias afterwards, as it might be too large for some instances to be used depending on the application. Alternatively, consider PUF 1 and PUF 2 but this time we set a different threshold between different challenges and different instances. For example, in the case of a strong PUF [1], used in identification protocols, the library is immense (with 2^{128} available challenges) and changes for each instance. This scenario allows us to minimize the bias of each response for each PUF instance. As shown on Fig. 2 the FHDs of these PUF 1^* and PUF 2^* are close to the previous PUF 1 and PUF 2 FHDs, but are completely unbiased and show better results in the NIST tests.

We demonstrate the performance of a high-speed CMOS-compatible integrated photonic architecture used as a PUF without major overheads on the post-processing side. The large library and the performances of PUF 1^* and PUF 2^* show the potential of this architecture. Still, an increase in behavioral complexity is necessary given the current results for the Approximate Entropy result.

References

1. F. Pavanello *et al.*, "Recent advances in photonic physical unclonable functions," in *2021 IEEE European Test Symposium (ETS)*, pp. 1–10, IEEE, 2021.
2. B. T. Bosworth *et al.*, "Unclonable photonic keys hardened against machine learning attacks," *APL Photonics*, vol. 5, no. 1, p. 010803, 2020.
3. L. van der Hoeven *et al.*, "Ring resonator networks as physical unclonable keys," in *Integrated Photonics Research, Silicon and Nanophotonics*, pp. IM3B–2, Optica Publishing Group, 2022.
4. Z. Lu *et al.*, "Performance prediction for silicon photonics integrated circuits with layout-dependent correlated manufacturing variability," *Optics express*, vol. 25, no. 9, pp. 9712–9733, 2017.
5. C. Marchand *et al.*, "Implementation and characterization of a physical unclonable function for iot: A case study with the tero-puf," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 1, pp. 97–109, 2018.