Photonic Physically Unclonable Functions using Ring-Assisted Contra-Directional Couplers

Mohammad Amin Mahdian,[1] Ebadollah Taheri,[1]
Kaveh (Hassan) Rahbardar Mojaver,[2] and Mahdi Nikdast[1*]

[1] *Electrical and Computer Engineering Department, Colorado State University, Fort Collins, Colorado, USA*
[2] *Department of Electrical and Computer Engineering, McGill University, Montréal, QC, Canada*

[*] *Mahdi.Nikdast@colostate.edu*

Abstract: We demonstrate a novel silicon-photonic-based Physically Unclonable Function (PUF) using grating-assisted contra-directional couplers integrated with perforated microring resonators. In the worst-case scenario, our device exhibits at least a 0.18 Hamming distance from the destined PUF.

1. Introduction

The rapid expansion of communication networks necessitates varying levels of security across each layer, from the application to the physical layer. Different security methodologies have been proposed and implemented, including end-to-end encryption, secure socket layer, virtual private networks, and admission control [1]. In addition, securing devices at the physical layer is essential to prevent physical-layer attacks, such as tampering and jamming [1]. Various methods for generating keys to enhance physical-layer security have been explored, such as Quantum Key Distribution (QKD) and Digital Signal Processing (DSP). However, these approaches often prove to be ineffective in providing cost-effective and unclonable solutions. Physically Unclonable Functions (PUFs) offer a unique approach by utilizing fabrication features to store information within their physical characteristics.

A robust PUF possesses distinctive features crucial for secure applications [1, 2]. It must be reproducible, consistently generating the same responses for a given input or challenge. Also, its responses must be uniquely identifiable, making each PUF instance distinct. Uncloneability is fundamental, ensuring responses cannot be duplicated even with detailed knowledge of the PUF's structure or behavior. PUFs should operate in a one-way fashion, preventing the reconstruction of the original challenge from the response. Furthermore, their responses should be unpredictable by adversarial attacks, such as those based on machine learning (ML), introducing uncertainty and enhancing security. Lastly, PUFs should exhibit tamper-evident characteristics, making any malicious interference easily detectable, thus upholding the overall integrity of the system. These combined features define the core attributes of a reliable and effective PUF [3], considered at the core of the implementations in this work.

To introduce optical PUFs in integrated photonic systems, it is essential to implement them based on Silicon Photonic (SiPh) devices and their functions to overcome the challenges of existing PUFs relying on bulkier materials and camera-detection methods [3]. In this paper, we design a new optical PUF based on the principles of grating-assisted Contra-Directional Couplers (CDCs) integrated with Perforated Microring Resonators (P-MRRs). The incorporation of CDC into our optical PUF design is particularly advantageous due to the large and complex design space they offer and their non-uniform sensitivity to different fabrication-process variations. The addition of P-MRRs introduces an additional nonlinearity to the response of optical pathways in CDCs while inherent randomness in the sub-feature size holes within the rings adds an extra layer of complexity. This work underscores the potential of CDCs as a novel and effective tool for enhancing hardware security in integrated photonic systems.

2. Design PUFs based on Silicon Photonic Contra-Directional Couplers

CDCs are widely used in the design of optical add-drop filters due to their wideband response. A basic CDC structure consists of two waveguide gratings that are placed in proximity (see Fig. 1(a)). The phase match condition in a CDC can be defined as $\beta_1 + \beta_2 = \frac{2\pi}{\Lambda}$, where $\beta_{1,2}$ are the propagation constants of the coupled modes of the first and second waveguides, and Λ is the period of perturbations [4, 5]. To reduce the directional coupling in CDC structures, the two waveguides are designed to have asymmetrical widths. In Fig. 1(a), we have showcased a CDC structure and its drop response. In this work, to create a more complex response from the through and add port, we considered the same waveguide widths for the two grating structures, hence reducing the contra-directional coupling coefficient, and creating a response similar to a mix of directional and contra-directional couplers. The CDC structure offers a complex design space that can be utilized to complicate the PUF behavior, such as the gap between the two gratings, the period of the gratings (Λ), widths of the waveguides ($W_{1,2}$), congregation depths ($\Delta w_{1,2}$), and the number of gratings (N), as shown in Fig. 1(a). We have presented a response of a CDC structure operating in C-band (1530–1560 nm) in Fig. 1(b). Prior work showed how a small mismatch between the periods of the grating ($\Lambda_{1,2}$) can create nonlinear behavior in the response of different CDCs [6]. In addition, CDCs possess many sharp corners on their grating teeth that will experience rounding effects during the fabrication

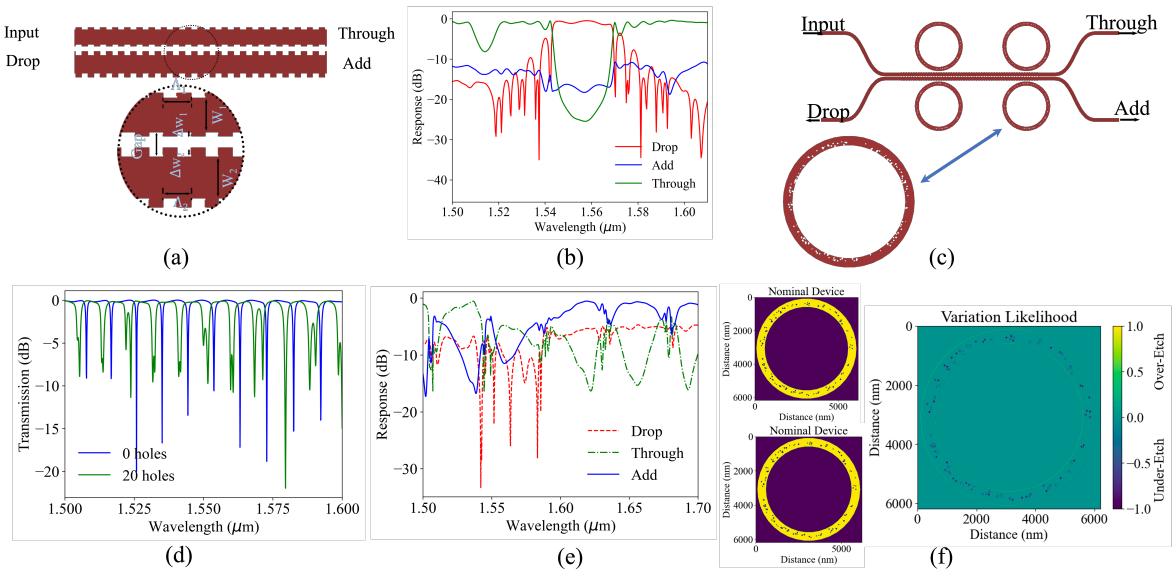

Fig. 1. (a) CDC structure and design parameters. (b) Response of a CDC structure operating as an add-drop filter. (c) The proposed PUF structure and a P-MRR. (d) Through-port response of 10-μm radius P-MRR with 20 random holes. (e) Response of the different ports of the proposed PUF. (f) Demonstration of the predicted P-MRR structure after fabrication using Prefab [9].

process, which will compromise the coupling efficiency of the structure. However, corner rounding effects can be predicted (to some extent, i.e., systematic variations) using optical lithography models. Therefore, we did not consider them in our work and focused on variations with a more random nature (e.g., line-width variations).

Furthermore, to add more complexity to the response of our CDC structure, we couple four randomly perforated MRRs to the coupling region of CDC (see Fig. 1(c)). The random placement of the holes on the rings causes a random shift and deformation in the resonance of the rings [7]. This creates an unpredictable resonance behavior that is indicated in Fig. 1(d), for a through-port response of a 10 μm radius ring with 20 holes. Fig. 1(e) shows the response of a PUF for all three ports. The holes on the ring have radii ranging from 30 to 60 nm, and they are created at various random distances from the inner edge to the outer radius of the ring. Due to the random nature of the hole placement, in some instances, the holes are positioned closely to each other, creating larger cavities within the ring. This further enhances the unclonable nature of the physical structure. For this work, we assume that all the holes in the ring are filled with silicon dioxide. However, if the radius of the rings becomes smaller than the minimum manufacturing feature size, the holes may not be completely filled with oxide, leaving air gaps within the structure and further making the impact of the manufacturing process on the rings inconsistent [8].

We used Prefab [9] deep learning-based prediction model to predict the fabricated structure of these rings. Fig. 1(f) shows the designed layout and the predicted layout of the structure after fabrication. It can be observed that in some cases, the holes are not etched entirely and create a asymmetrical shape enhancing the sensitivity of these devices to fabrication-process variations. Fig. 1(f) shows an example of a P-MRR structure prediction. We can see from the variation likelihood graph that most of the perforations will be most likely under-etched after fabrication. Note that this may change across different fabrications (e.g., the predicted fabrication models used based on Prefab [9] aligns with Applied Nanotools Inc. process).

To evaluate the performance of the proposed PUF, we performed FDTD simulations based on different designs and different variations of the same design. Different designs of the PUF have completely different radii for P-MRR and also the number of the gratings and their period. For different design variations, to mimic the impact of random process variations in our simulations, we considered the same device but changes in distribution and placement of the holes on P-MRR and ± 1 to 5 nm shift in the grating period and ± 10 to 30 nm shift in the gap between the grating and P-MRR.

3. Key Extraction and Evaluations

In the authentication system (depicted in Fig. 2(a), we assume a challenge-response library, enabling the random selection and application of challenges to the token. One challenge is shown in Fig.2(b) as an example, which is created as sequences of 1-ns pulses spanning six different wavelengths. The combination of the time series and wavelengths elevates the complexity and security of our authentication process. When a challenge is presented, the token generates a unique analog response, which is subsequently digitized for evaluation, shown in Fig. 2(c).

We opted to utilize the response from the add port due to its broader bandwidth in comparison to the through

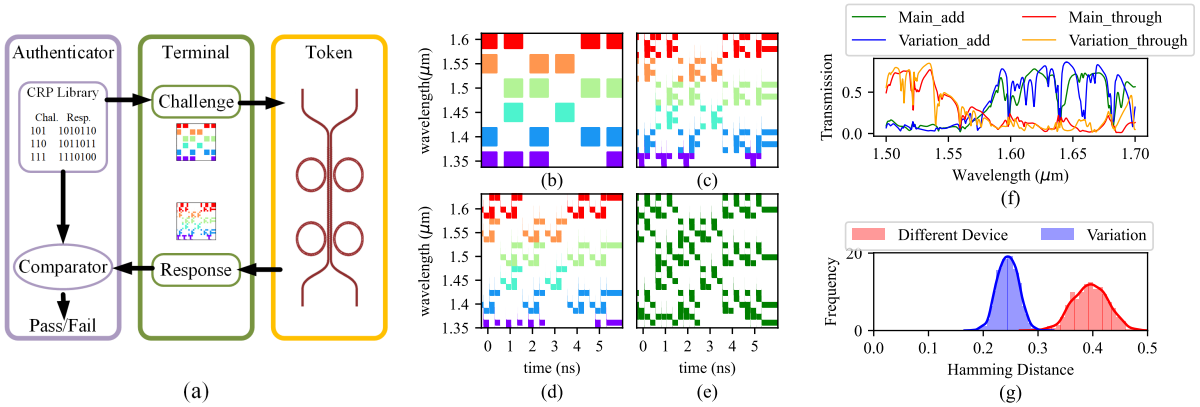

Fig. 2. (a) The authentication system. (b) A challenge sample comprising 6 series of pulses spanning 6 different wavelengths. (c) The response of the primary device to this challenge. (d) The response of a device variation. (e) XOR result of the two responses, with green points indicating discrepancies between the primary device and the variation. (f) Transmission characteristics of the main device and the variation under different wavelengths. (g) The distribution of Hamming distances between the main device and its variation, as well as a different device, over 1000 authentication trials.

port. It is worth noting that a combination of responses from both the through and add ports, such as XORing the responses, can be employed to achieve a greater level of key complexity. However, it is essential to consider that this approach comes with the added cost of requiring more connections between the token and the terminal.

The digitized response of the add port is then compared to the expected response associated with the challenge. Successful authentication occurs when these responses align within a predefined threshold. For instance, in Fig. 2(d), we observe the response of a device variation, while in Fig. 2(e), the XOR of the two responses is presented, with discrepancies highlighted by green points. These discrepancies, signified by the green points, play a crucial role in distinguishing between the primary device and the variation. This distinction enables the authenticator system to differentiate between the two tokens and appropriately reject authentication when necessary. This secure authentication process forms a pivotal feature of the proposed optical PUF design, enhancing the overall security and access control of the system. Transmission characteristics under different wavelengths are shown in Fig. 2(f), illustrating the uniqueness of the device's performance in a range of scenarios.

In our evaluations (shown in Fig. 2(g)), we thoroughly examined the optical PUF against various scenarios, including device variations and comparisons to distinct devices. We conducted a series of 1000 authentication challenges, leading to the distribution of Hamming distances. The consistent minimum Hamming distance of 0.18 across all 1000 authentication trials, even when considering variations within the same device or comparing with a different device, is compelling evidence of the robustness and reliability of our optical PUF design. It reaffirms its ability to maintain a secure and distinctive authentication process, resilient to environmental and device-related variables. Evaluations using ML prediction models are not included and will be presented in our future work.

4. Conclusion

We presented a novel optical PUF design with CDC integrated with P-MRRs, to provide robust physical-layer security. The key extraction and evaluation process effectively authenticates tokens, in the presence of fabrication-process variations. Our work shows the promise of CDCs to create efficient PUFs in integrated photonic platforms.

References

1. P. N. Goki *et al.*, "Optical identification using physical unclonable functions," arXiv:2305.02141 (2023).
2. J. He and othres, "DSP-based physical layer security for coherent optical communication systems," IEEE Photonics J. **14**, 1–11 (2022).
3. B. C. Grubel *et al.*, "Silicon photonic physical unclonable function," Opt. Express **25**, 12710–12721 (2017).
4. W. Shi *et al.*, "Silicon photonic grating-assisted, contra-directional couplers," Opt. express **21**, 3633–3650 (2013).
5. L. Tunesi *et al.*, "Thermal control scheme in contra-directional couplers for centered tunable bandwidths," in *IEEE International Conference on Numerical Simulation of Optoelectronic Devices (NUSOD),* (2023), pp. 115–116.
6. M. A. Mahdian *et al.*, "Bandwidth-adaptive single- and double-channel silicon photonic contra-directional couplers," in *IPC,* (2023).
7. M. Gabalis *et al.*, "A perforated microring resonator for optical sensing applications," J. Opt. **16**, 105003 (2014).
8. H. Shiran *et al.*, "Impact of SiO2 cladding voids in SiPh building blocks," in *IPC,* (2020), pp. 1–2.
9. D. Gostimirovic *et al.*, "Improving fabrication fidelity of integrated nanophotonic devices using deep learning," ACS Photonics (2023).