scientific reports

Check for updates

OPEN

Hardware assurance with silicon photonic physical unclonable functions

Mohammad Amin Mahdian[1], Ebadollah Taheri[1], Kaveh Rahbardar Mojaver[2] & Mahdi Nikdast[1]✉

In the modern landscape of optical communication networks, ensuring robust security is increasingly critical, particularly for applications requiring seamless integration and minimal attack surfaces. Photonic Physical Unclonable Functions (PUFs) leverage the response from the photonic devices that are prone to inherent physical variations to generate unique and unpredictable signature identifiers which are then utilized by an authentication system for identification or encryption purposes. These photonic PUFs can be cohesively integrated into systems that use optical communication, whereas using electronic PUFs would introduce additional vulnerabilities due to the need for signal-domain conversions between optical and electronic signals. In this paper, we present the design, fabrication, and experimental evaluation of advanced silicon-photonic-based PUFs utilizing Contra-Directional Coupler (CDC) structures. These structures offer a complex design space and are intrinsically sensitive to fabrication-process variations, making them ideal for creating unique and secure responses. We introduce several innovative design enhancements, including randomized corrugation functions, perforated designs, and ring-assisted CDCs, to increase the complexity and unpredictability of the CDC response. Measurement results from the fabricated CDCs demonstrate their capability to achieve an average Hamming distance threshold of over 0.2, effectively distinguishing between legitimate devices and their copies. We rigorously tested these fabricated designs against three different machine-learning-based attack scenarios. The results showed a Hamming distance of over 0.4 with a standard deviation of less than 0.01 at a quantization level of three, using 10,000 samples of challenge-response pairs. These findings underscore the potential of silicon photonic PUFs in enhancing security for optical communication systems of different scales. The integration of such photonic PUFs offers robust and reliable security solutions for applications where traditional electronic methods introduce additional attack surfaces and fail to provide adequate protection.

Keywords Silicon photonic, Physical unclonable functions, Hardware security

Physical Unclonable Functions (PUFs) offer a promising approach to Physical Layer Security (PLS) by leveraging the inherent physical characteristics of each device to generate unique secret keys. These keys are derived from the structural features introduced by fabrication-process variations (FPVs), thereby eliminating the need for power-consuming memory storage and complex encryption algorithms. A crucial aspect of PUFs is that even if an attacker manages to acquire the secret key, replicating it is impractical. The uniqueness of each PUF key arises from the randomness FPVs and the intrinsic complexity of the PUF design, which makes exact duplication of the physical characteristics of a device nearly impossible. This inherent security feature significantly complicates any physical access attempts by attackers to extract or duplicate the keys[1].

While security at various levels, such as application, presentation, and network, has advanced rapidly, PLS remains complex due to the inherent challenges of designing efficient protocols at this level[2,3]. Current solutions often rely on non-volatile or battery-backed memories to store secret keys, utilizing digital signatures or encryption[4,5]. For instance, flash memory and Electrically Erasable Programmable Read-Only Memory (EEPROM) are commonly used for key storage due to their ability to retain data without power[5]. However, while non-volatile memories are generally efficient in data retention, they can require significant power during write operations and have slower write speeds compared to volatile memories. Additionally, these methods require complex designs and remain vulnerable to modeling attacks, necessitating additional preventive circuitry[6].

[1]Electrical and Computer Engineering Department, Colorado State University, Fort Collins, CO, USA. [2]Department of Electrical and Computer Engineering, McGill University, Montreal, QC, Canada. ✉email: mahdi.nikdast@colostate.edu

PUFs are security primitives that exploit the inherent physical variations in manufacturing processes to generate unique responses to external challenges. These variations, which are extremely hard to replicate exactly, form the basis of a PUF's security. PUFs are classified into two main types: weak and strong. Weak PUFs produce a limited number of challenge-response pairs (CRPs), which makes them less secure because their responses can potentially be predicted or modeled by an attacker. In contrast, strong PUFs can generate a vast number of CRPs, making them significantly more secure. This large pool of CRPs ensures that even if an attacker observes some responses, it remains infeasible to predict the responses to new challenges[7].

Using electronic PUFs in optical communication introduces vulnerabilities due to the need for signal-domain conversions between optical and electronic signals. This highlights the need for alternative solutions that eliminate such conversions. Silicon photonics (SiPh) technology enables the integration of optical functionalities into integrated circuits using standard CMOS processes. In particular, it is possible to leverage the unique FPVs in SiPh fabrication to create photonic PUFs that can directly benefit optical communication systems. SiPh devices are an example of strong PUFs. They offer higher security due to their ability to generate a large number of CRPs, making them more resistant to enumeration attacks[7]. The integration of SiPh PUFs with CMOS processes is particularly beneficial for security. This compatibility with CMOS technology means that the PUFs and their electronic measurement circuitry are fabricated on the same chip. This co-integration prevents the physical separation of the PUF from its control and readout electronics, thereby complicating any unauthorized physical access or tampering. As a result, attackers cannot easily isolate the PUF to analyze or clone it, significantly enhancing the overall security of the device[1,6]. As an example, Fig. 1 shows the operation of a photonic PUF and how it is used for authentication for satellite optical communication.

Furthermore, in scenarios like satellite communication, where devices are exposed to harsh environments and radiation, traditional electronic security measures may falter[8]. Photonic PUFs can be considered as an alternative solution[9] by leveraging the unique properties of photonics to ensure secure authentication and data transfer, specifically in optical communication systems where the use of electronic PUFs necessitates signal-domain conversions. These photonic PUFs can offer advantages in optical communication, where their passive nature can provide power saving and reduce system design complexity, ensuring reliable security by reducing the attack surfaces. Some prior work demonstrated the robustness of passive SiPh devices (like ours) under high total ionizing doses (TID)[9,10]. While our work focuses on the innovative design and performance of SiPh PUFs, further tests and experiments are necessary to rigorously validate their robustness under radiations, which will be the focus of our future work.

Earlier SiPh PUF designs faced challenges with non-integrated structures that compromised security and packaging. Recent advancements have focused on integrated SiPh PUFs using microdisk cavities[11], Mach–Zehnder interferometers (MZIs)[12,13], microring resonator (MRR) arrays[14], and quasi-crystal structures in Michelson-type interferometers[15]. These designs, although innovative, often had large footprints, relied on active circuitry, or utilized ultrafast nonlinear optical interactions which add significant complexity to the design and operation of the PUFs. These effects require precise control over input power levels and can complicate the integration of these PUFs into standard optical communication systems.

In this work, we present a pioneering PUF design utilizing Contra directional Couplers (CDCs) that harness numerous physical features highly sensitive to FPVs, without the need for nonlinear silicon effects. Previously, we introduced the concept of an unclonable function based on CDCs in[16] and demonstrated their potential for generating unique, unclonable keys. Building on this foundational work, we now provide experimental validation and explore various innovative designs further to enhance the security and functionality of CDC-based PUFs.

In this work, we propose and fabricate several design techniques aimed at extracting unclonable responses. These techniques include the use of apodization functions to modulate the coupling coefficient, perforation of structures to introduce random variability, integration of MRR-assisted structures, and combinational methods that leverage these elements together. Each design was meticulously fabricated and experimentally validated to assess its performance. To evaluate the effectiveness of these designs, we implemented an authentication system that validates the generated keys from the experimentally measured responses of the proposed PUFs. From five fabricated copies of each photonic PUF design, we extracted 10,000 binary keys, demonstrating their

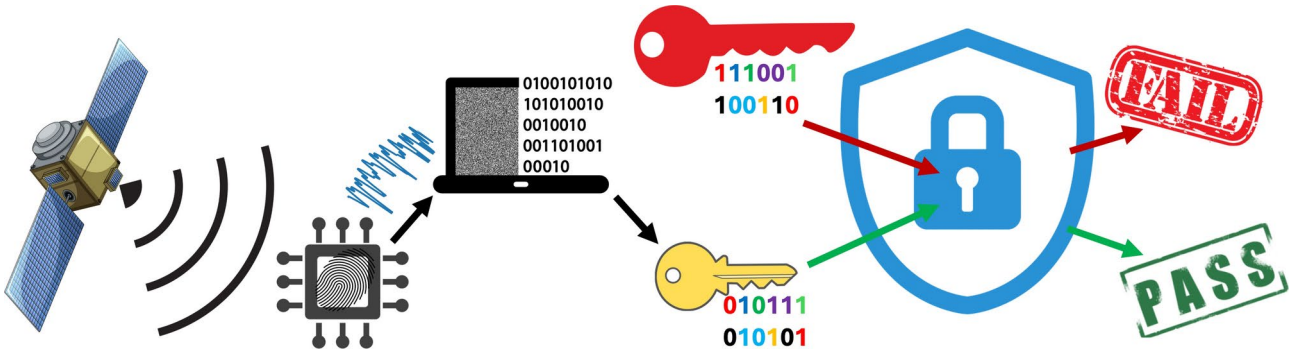

Fig. 1. An example of a photonic PUF used for secure key generation in satellite optical communication. Only legitimate responses to satellite challenges are authenticated, ensuring secure access. If the response is not legitimate, the connection is denied.

uniqueness and reproducibility. Furthermore, we subjected these designs to rigorous testing against three state-of-the-art machine-learning-based attack scenarios[17–19]. Our results underscore the robustness of the proposed PUF designs, showcasing their potential for secure key generation in SiPh applications. This comprehensive analysis highlights the promising application of CDC-based PUFs in enhancing security in applications where traditional electronic PUFs may fall short.

Device design and analysis

Contra directional couplers

SiPh CDCs are four-port devices comprising two dissimilar waveguide grating structures placed in proximity to form a coupling region that functions as a wavelength-selective add-drop filter (see Fig. 2a). In a conventional design, the two waveguides have different widths ($W_1 \neq W_2$) to suppress co-directional coupling due to the phase mismatch between their propagation constants[20]. The grating pitch (Λ) must be designed to satisfy the phase match condition given by:

$$\Lambda_D = \frac{2\pi}{\beta_1 + \beta_2}, \tag{1}$$

where Λ_D is the perturbation period of the CDC, and β_1 and β_2 are the propagation constants of the forward and backward propagating fundamental transverse electric (TE) modes of the coupler, respectively. The bandwidth of CDCs is highly sensitive to the corrugation widths ($\Delta w_{1,2}$), with small variations in these widths significantly affecting the bandwidth. These sensitivities arise from the limitations of the lithography process, including smoothing and proximity effects that alter the precise geometries of finely featured SiPh devices[21].

The design parameters of a CDC are illustrated in Fig. 2. The structure of a CDC is characterized by several key parameters: grating pitch ($\Lambda_{1,2}$), the gap between the waveguides, corrugation widths ($\Delta w_{1,2}$), and waveguide widths ($W_{1,2}$). These parameters collectively define the behavior and performance of the CDC including the bandwidth[22], shape of the sidelobes[23], central wavelength[24], and the number of drop-port channels[25,26]. Subtle changes in these geometric parameters can significantly influence the mode profile and, consequently, the coupling coefficient of the CDC, as described by:

$$\kappa = \frac{\pi \Delta\lambda}{\lambda_0^2}\left(\frac{n_{g1} + n_{g2}}{2}\right). \tag{2}$$

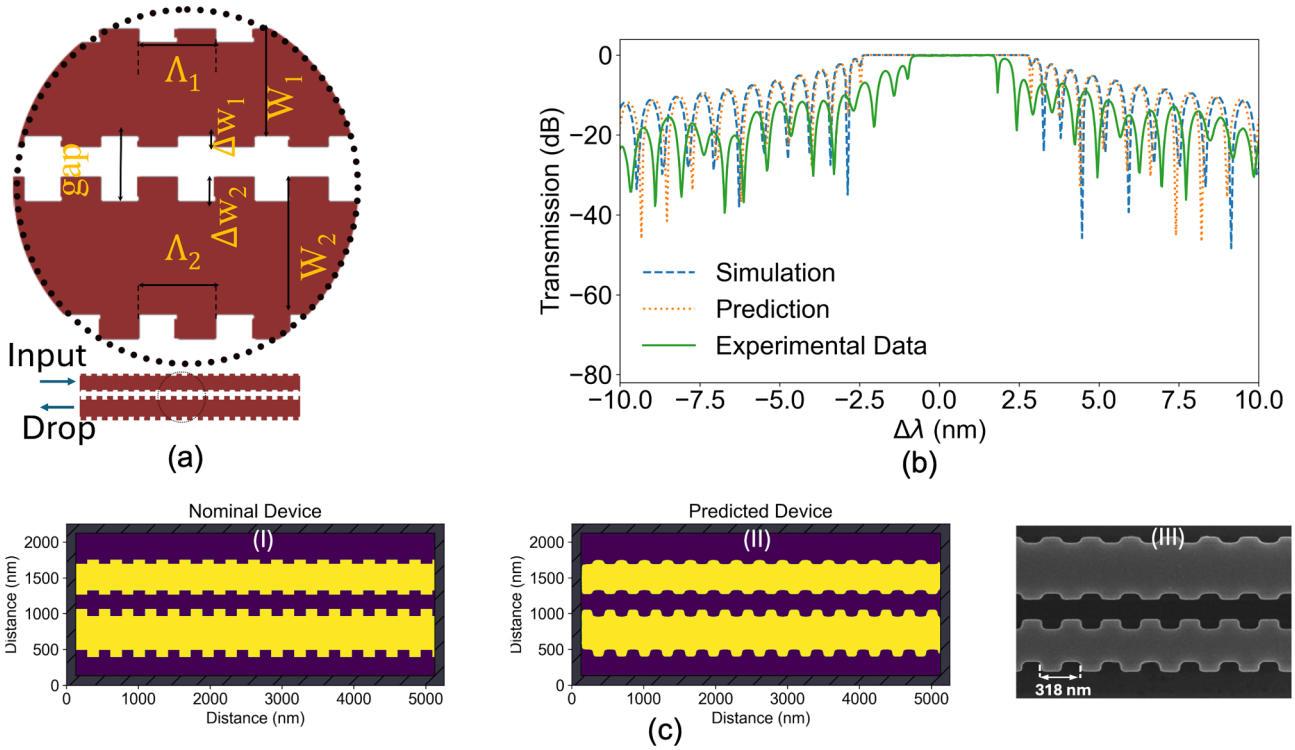

Fig. 2. (**a**) Schematic illustration of a CDC indicating its design parameters. (**b**) Comparison of simulated, AI-predicted, and fabricated devices. (**c**) Layout of (I) the nominal device, (II) the predicted device using prefab, (III) and the SEM image of the fabricated device.

In this equation, κ is the coupling coefficient, $\Delta\lambda$ is the wavelength shift, λ_0 is the central wavelength, and n_{g1} and n_{g2} are the group indices of the coupled modes of the first and second unperturbed waveguides, respectively. Note that the coupling coefficient directly affects the bandwidth of the CDC.

The effective indices of the two waveguides (n_1 and n_2), the grating pitch (Λ_D), and the modulation depth of the grating ($\Delta w_{1,2}$) all play crucial roles in shaping the sidelobe formation around the main drop channel response and determining the central response wavelength of the CDC. Variations in these parameters can lead to changes in the spectral characteristics of the device, influencing its overall performance in applications such as wavelength-selective filtering.

Precise control over these design parameters is essential for optimizing the CDC's performance. The gap between the waveguides affects the interaction strength between them, while the grating pitch must be carefully tuned to achieve phase matching. Similarly, the corrugation widths and waveguide widths must be optimized to balance the trade-offs between coupling efficiency, bandwidth, and sidelobe suppression. Mastering these design elements allows for the creation of highly efficient and customized CDCs tailored for specific photonic applications, including generating responses suitable for robust PUFs.

In Fig. 2b, we compare the drop-port transmission of a simulated CDC device with a grating period of 318 nm, waveguide widths of $W_2 = 560$ nm, and $W_1 = 430$ nm, and a gap of 200 nm, against a fabricated device. The fabricated device exhibits a lower bandwidth compared to our simulation results. This discrepancy is primarily due to lithography errors, which affect the precision of the CDC's grating teeth, thereby reducing the coupling coefficient, which is dependent on the waveguide's effective index. The comparison includes the drop port transmission of three types of CDCs: one of our fabricated devices through Applied Nanotools[27], a nominal CDC, and a 2D AI-predicted device[28]. The AI-predicted model aims to estimate the post-fabrication performance based on training data from the same foundry used for our devices. We have shown these 3 different devices in Fig. 2c. Our analysis reveals that the fabricated device's bandwidth is reduced by 3 nm compared to the nominal design. In contrast, the AI-predicted model shows only a 1 nm reduction in bandwidth. This discrepancy highlights the limitations of the AI model, which, despite its predictive capabilities, cannot fully capture all post-fabrication imperfections. These include corner rounding, as illustrated in Fig. 2c-II, variations in device thickness, and uneven lithography effects along the length of the device.

Optical lithography imperfections can cause deviations in the grating period and waveguide dimensions, directly impacting the coupling efficiency and the overall performance of a CDC. Specifically, over-etching can reduce the width of the waveguides, resulting in a weaker coupling coefficient than predicted by theory and leading to a reduction in bandwidth. Additionally, variations in the thickness of the waveguides can cause changes in the effective index, further affecting the device's spectral response. Fabricated devices have experienced uneven changes in width, exacerbating these issues. Although AI-predicted models can anticipate and compensate for some minor deviations, providing a closer approximation to the ideal bandwidth, they are not immune to the challenges posed by the intricate nature of CDCs. Even small lithographic imperfections can have a pronounced impact on the CDC's bandwidth and sidelobe characteristics highlighting the sensitivity of CDCs to FPVs.

Fabrication-variation enhanced CDC structures

To enhance the complexity and unpredictability of the CDC response, we have employed four design approaches: (1) Randomized corrugation functions, (2) Perforated designs, (3) MRR-assisted CDCs, and (4) A combination of these methods. Additionally, we integrated previously introduced design techniques, such as apodization[29] and two-period gratings[25], to further increase the complexity of CDCs. These approaches leverage the geometric parameters of the CDC to manipulate the drop-port response, enabling the generation of unclonable keys that encapsulate user information within their physical features. We discuss each of the design methods considered in the following.

Randomized corrugation design involves intentionally varying the depth of the CDC corrugations, which in turn randomly alters the coupling coefficient. This random variation causes the sidelobes of the main channel to create a nonuniform pattern, unlike wavelength division multiplexing (WDM) applications where CDCs are typically apodized to reduce the sidelobes of the spectral response. In this method, the grating teeth are gradually increased to achieve stronger coupling at the central spectral channel response. This randomization disrupts the drop-port response, which can then be utilized to extract unique features to create a robust PUF.

To investigate the effect of random corrugation depth on a CDC, we used the transfer matrix method (TMM)[20,29] to estimate this effect on a CDC with the same dimensions as the design presented in Fig. 2. Figure 3a shows the drop-port transmission of the simulated and fabricated devices. The main channel bandwidth is decreased due to the non-uniform variation of the coupling coefficient. Random corrugation depth can fall below the minimum feature size of the fabrication process. This is depicted in Fig. 3b, where Δw is shown as a function of the number of gratings. The lower limit of Δw is set to 10 nm, and the higher limit is 100 nm. When Δw is less than 50 nm, the correlation appears as a smooth wave. This causes the fabricated device to miss subtle features that exist in the nominal device.

Specifically, the non-uniform coupling coefficient leads to an asymmetrical spectral response, characterized by reduced bandwidth and altered sidelobe patterns. By comparing Fig. 3c and d, we can see how some sections of the device have very different silicon profiles. These variations allow us to use these features as a method for creating new identities from these devices.

Perforated designs employ features with dimensions below the minimum feature size of the technology. The minimum feature size of the fabrication process process is 60 nm meaning that the devices with features smaller than 60 nm may not be fabricated reliably[27]. To further use this limitation we introduced holes with sub-feature

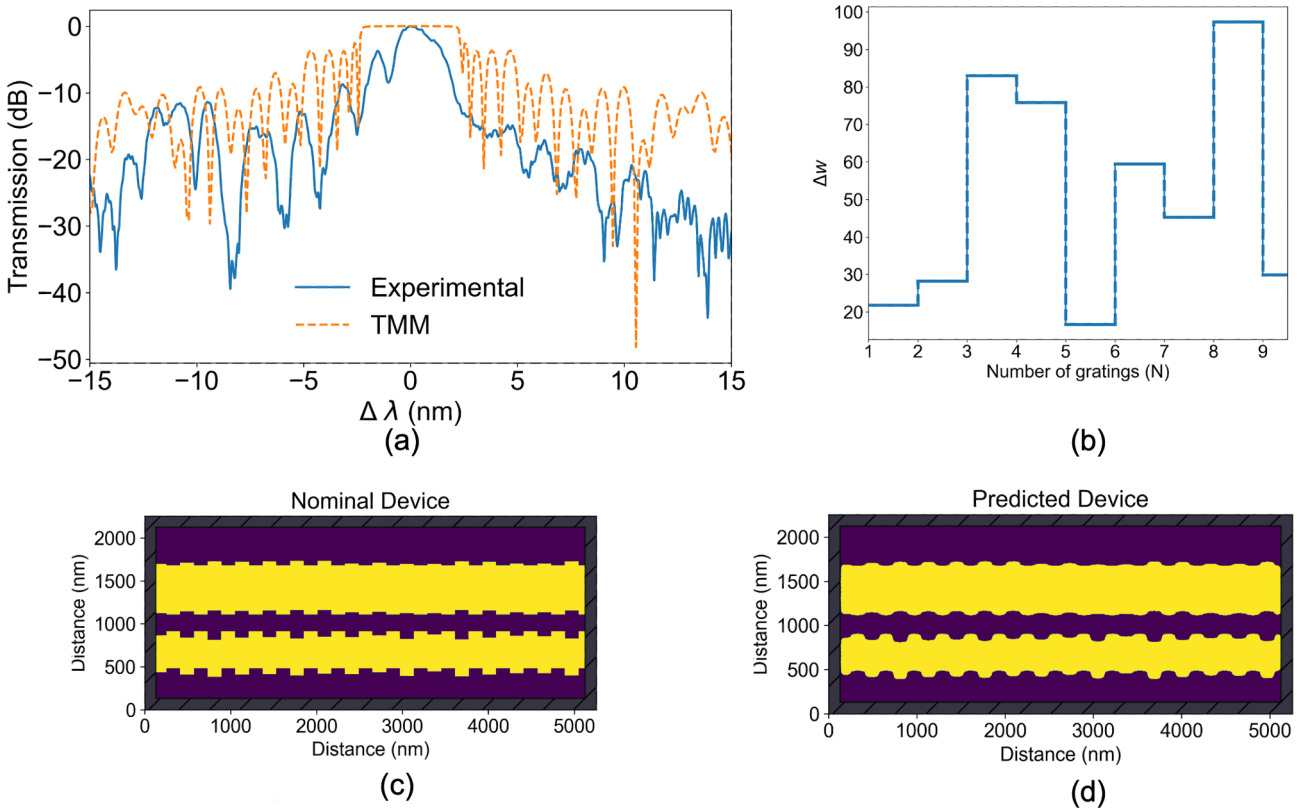

Fig. 3. (**a**) TMM modeled and experimentally measured drop-port transmission of a randomly corrugated CDC. (**b**) Corrugation depth of one grating waveguide as a function of the number of grating in randomized corrugation device. (**c**) Layout of a nominal randomly corrugated CDC. (**d**) The AI-predicted layout of the device shown in (**c**).

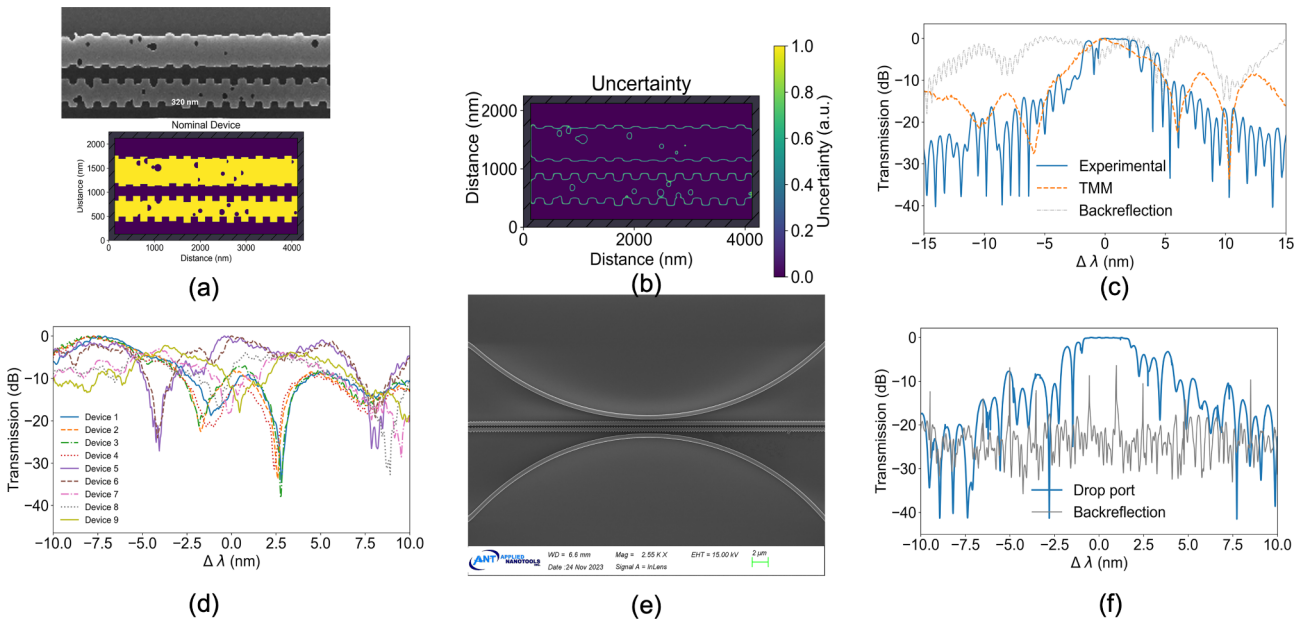

Fig. 4. (**a**) A comparison between the fabricated and nominal perforated device. (**b**) The uncertainty of the AI-model prediction on this device. (**c**) Response of a perforated and a normal CDC with the backreflection response of the perforated CDC. (**d**) A comparison between the responses of nine perforated designs. (**e**) SEM image of an MRR-assisted CDC. (**f**) The response of the MRR-assisted the CDC with its backreflection.

size geometries over the different sections of the CDCs. The introduction of holes to CDCs is done with random distribution in both the placement and size of the hole.

A perforated CDC with random hole placement is demonstrated in Fig. 4a. The top figure shows the SEM image of a fabricated device and the bottom figure shows the layout of the nominal device. Figure 4b shows the uncertainty of the AI prediction in the prediction of this device. The most significant uncertainty is observed at the CDC's perimeter and the etched holes' inner surface. In Fig. 4c we can observe the drop-port transmission of both a standard CDC and a perforated CDC, along with the back reflection of the perforated design. The back reflection in the perforated design primarily arises from the abrupt change in the refractive index. This occurs because the holes are filled with silicon oxide, or in some cases, these holes may remain as void air gaps due to their sub-feature size[30].

The perforated design of the CDC undergoes more FPVs due to its intricate structure. This design has numerous small features, which makes it more sensitive to imperfections during the fabrication process. Variations in the etching depth, sidewall roughness, and uniformity of the perforations can significantly impact the optical properties of the device. As a result, these fabrication inconsistencies cause changes in the response of the drop port of these devices. Specifically, the slight differences in the physical structure of the perforated CDCs lead to variations in how light is transmitted through the device. These variations can affect the performance metrics such as insertion loss, bandwidth, and overall efficiency.

In Fig. 4d, we compare the responses of multiple fabricated perforated CDCs. Devices 1 to 4 are identical copies of the perforated CDC, each with a period of 320 nm and the same hole distribution. Devices 5 and 6 represent the drop-port response of a perforated CDC with the same period but a different random hole distribution. Devices 7 to 9 are identical copies of a perforated CDC with a period of 318 nm. The results demonstrate that even subtle changes in the hole distribution or the grating period can significantly impact the drop-port response. This sensitivity to fabrication variations is crucial for PUFs, which rely on unique and unpredictable responses to ensure security. By varying the hole distribution and grating period, we can enhance the complexity and diversity of the CDC responses. This creates a large set of distinct and unclonable responses that are ideal for generating robust PUFs.

Additionally, the back reflection of these CDCs, although not the primary focus of this study, can be utilized to develop more complex authentication processes. The back reflection provides another layer of information that can be leveraged to further increase the complexity and security of PUF-based authentication systems. However, in this work, we focus solely on the drop port responses for simplicity and clarity in evaluating the potential of CDCs for PUF applications.

MRR-assisted CDCs combine the design of CDCs with MRRs. MRRs are known to suffer from FPVs. On average, these variations can cause a resonant-wavelength shift of approximately 2 nm with a single nanometer change in waveguide thickness. This sensitivity is due to FPVs stemming from optical lithography imperfections[31].

In the MRR-assisted CDC design, we combine the sensitivity of both the MRRs and the CDCs to generate a highly unique response at the drop port of the CDC. The MRRs exhibit high sensitivity to small changes in their physical dimensions and refractive index caused by FPVs. This sensitivity is utilized to enhance the security of the PUFs by making the optical response highly dependent on these unique and unpredictable variations.

By combining these two devices, the MRR-assisted CDC design amplifies the overall sensitivity to FPVs, making the response at the drop port extremely dependent on the precise geometrical and material characteristics of the device.

Figure 4e shows an SEM image of a fabricated MRR-assisted CDC structure, with its drop-port response demonstrated in Fig. 4f. By observing the back reflection of this device, we can see that the free-spectral range (FSR) of the reflection is 1.52 nm. The schematic of the device is presented in Fig. 5a. The largest ring in this structure has a radius of 35 μm. Based on the calculated FSR, the group index (n_g) for this ring is determined to be 8. This result indicates a slow light effect in the backward propagating mode in the CDC, as the group velocity, defined by $v_g = c/n_g$ (where c is the speed of light and n_g is the group index), is reduced[32].

Combinational devices combine different design methods that we discussed earlier. It includes a combination of MRR-assisted CDCs, perforated CDCs, and random perturbation of CDCs.

Figure 5b demonstrates a fabricated CDC with perforated MRRs placed in proximity to the CDC with a gap of 200 nm. As a different design, we have performed perforation on both MRR and CDC, as shown in the SEM image in Fig. 5c. The responses of these two devices are depicted in Fig. 5d and e, respectively. Additionally, Fig. 5d includes the response of a CDC without any MRR for comparison along with the backreflection of each device.

The results indicate that the presence of MRRs primarily affects the sidelobes rather than the main channel. This observation is likely because the rings used in the design are terminated at the drop port, which prevents significant peaks in back reflection. In contrast, Fig. 5e shows a stronger back reflection and decreased power transmission due to the perforations on both the CDC and MRRs. In this configuration, the MRRs are not terminated, leading to the observed back reflection.

Furthermore, the impact of termination is evident in Fig. 5f, which illustrates a device with perforations on both the CDC and MRR, but with terminated drop ports of the MRR. This termination results in reduced power transmission at the drop port, emphasizing the importance of termination in modulating device performance. The comparison highlights the critical role of both perforation and termination in managing sidelobe suppression and back-reflection characteristics, demonstrating how these factors influence the overall device response. The unique responses generated by these variations are deeply tied to the specific fabrication process, making each device inherently unique and difficult to replicate. This dependence on precise manufacturing variations ensures robust security for sensitive applications.

In our designs, we utilized the design features of CDCs, focusing on the width and periodicity of the gratings. Typically, CDCs are designed with asymmetrical widths for the two waveguides to avoid in-band reflection

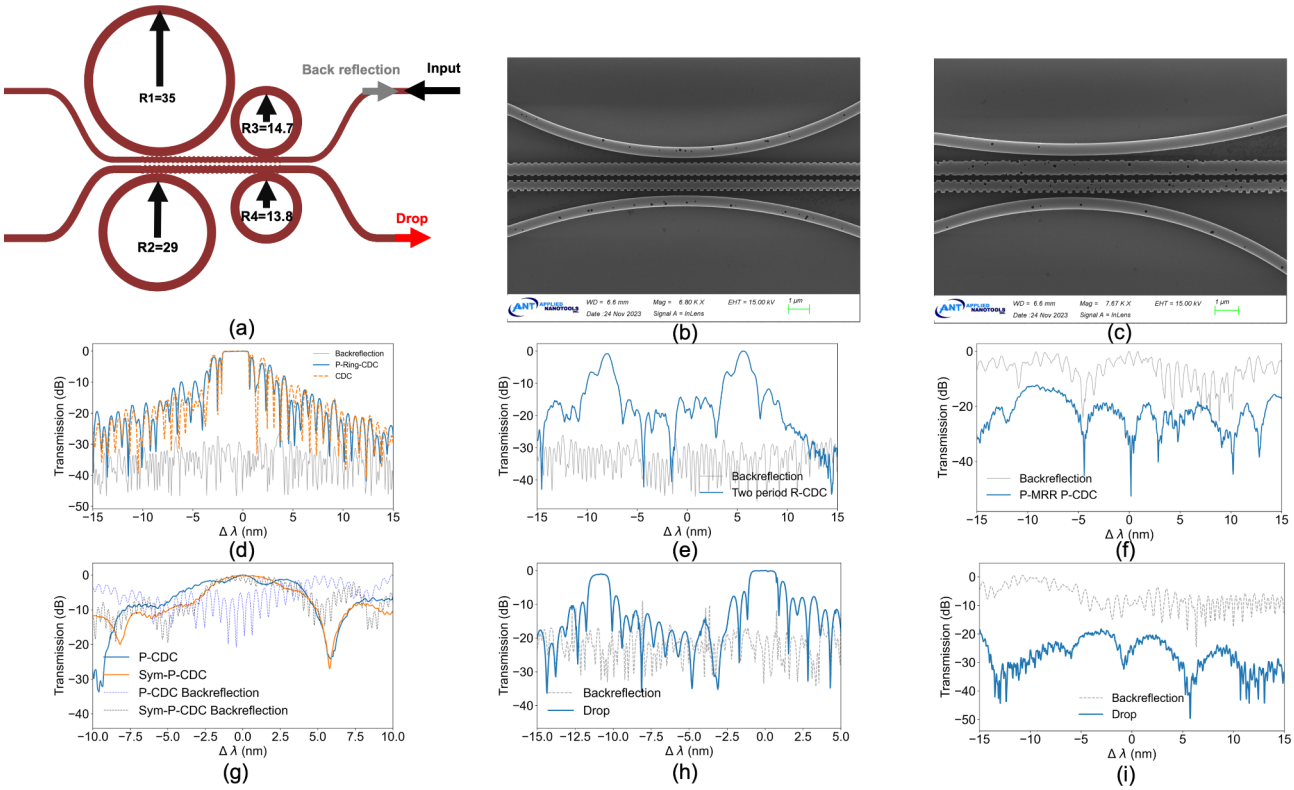

Fig. 5. (**a**) Schematic of an MRR-assisted CDC device whose drop port and backreflection are shown in Fig. 4f. (**b**) SEM image of a device with perforation only on the coupled rings (P-MRR-assisted CDC). (**c**) SEM image of a MRR-assisted CDC with perforation on both rings and the CDC (P-MRR P-CDC). (**d**) Response of a perforated MRR assisted CDC (P-MRR-assisted CDC) and a CDC without rings with the same design parameters. (**e**) Drop-port and backreflection response of an MRR-assisted two-period CDC with periods of 320 and 316 nm. (**f**) Drop-port and backreflection response of a perforated MRR assisted perforated CDC (P-MRR-assisted P-CDC) with a period of 320 nm. (**g**) Drop-port and back reflection response of a symmetrical CDC and drop-port response of an apodized CDC. (**h**) Drop-port and backreflection response of a two-period MRR-assisted CDC with non-terminated drop port on the MRRs. (**i**) Drop port and backreflection response of a two-period randomly apodized CDC.

from the grating structures. However, in some of our designs, we adopted symmetrical structures, resulting in both band reflection and directional coupling. Specifically, the width of both waveguides in the symmetrical structures was set to 450 nm. This design choice significantly impacts the main channel transmission and back reflection, as illustrated in Fig. 5g.

Furthermore, the figure demonstrates a device with hyperbolic tangent apodization. In the context of WDM applications, apodization is used to minimize sidelobes in the transmission spectrum of devices such as CDCs and optical filters. Sidelobes are secondary peaks in the transmission spectrum that can interfere with adjacent channels, causing crosstalk and reducing the overall performance of the WDM system. By employing apodization, the transition in the waveguide properties is made smoother, which significantly reduces the amplitude of these sidelobes, leading to cleaner signal separation and improved channel isolation. However, In the design of our devices, we performed the apodization to reduce the effective index of the grating waveguide by reducing the width. Causing a multiple-phase match condition to happen as the refractive index of the two granting coupler changes creating multiple peaks. The apodization described by the hyperbolic tangent equation:

$$\Delta w(n) = \frac{\Delta w_{\max}}{2}\left[1 + \tanh\left(\beta\left(1 - 2\left|\frac{2n - N}{N}\right|^{\alpha}\right)\right)\right],$$

where n is the grating number, N is the total number of gratings, $\Delta w_{\max}$ is the maximum change in width, and α and β are constants used to fine-tune the tapering profile. In this specific design, we used $\alpha = 2.8$ and $\beta = 5$.

By employing different apodization functions, we can generate unique device responses correlating with varying apodization parameters. This capability is essential for creating distinct device identities, a critical feature for photonic PUFs. The customized responses from these devices are crucial for applications in secure authentication, where unique and reproducible device characteristics are required. The incorporation of such

apodization techniques ensures that each device exhibits a highly specific and unclonable spectral response, enhancing the security and reliability of the photonic PUF.

In Fig. 5h, a two-period grating CDC structure coupled to MRRs is utilized. In this design, the two grating couplers have periods of 320 nm and 316 nm. The widths of the two waveguides are 570 nm and 430 nm, respectively. Four MRRs, each with a radius of 20 μm, are coupled to the CDC with two on each side. The drop port of the MRRs is left unterminated, allowing observation of the backreflection of the back-propagating mode coupled into the ring at the backreflection response of the device.

The two-period design of CDCs significantly enhances the uniqueness of PUFs. This design leverages the properties of two grating waveguides with different periods and waveguide widths, as depicted in Fig. 5i. For instance, the two grating waveguides in this configuration can either have different apodization functions or be randomly perturbed, as demonstrated in the figure. In this specific design, the gratings have periods of 320 nm and 315 nm with waveguides of 570 nm and 430 nm.

The distinct response observed in this design compared to previous ones is due to the absence of MRRs, leading to lower backreflection. The two-period CDC structure is particularly advantageous for PUFs because it combines the responses of two single-period gratings. According to Fourier analysis and numerical simulations, the output channels at the drop port can be designed independently and can have different bandwidths. Additionally, the integration of two-period CDCs in PUFs is beneficial for multiple reasons. The presence of two different grating periods enhances the complexity of the photonic response, making the system more secure and harder to replicate. This design provides the capability to filter two non-contiguous wavelength channels simultaneously, as each period corresponds to a specific drop channel. Experimental results have shown that the drop-port response of a two-period CDC structure is the superposition of the responses of the individual gratings, confirming the independent design of the output channels[25]. The implementation of two-period CDCs in PUFs allows for more compact device configurations without compromising performance. The ability to tailor the spectral properties of each filtered channel independently enhances the flexibility and robustness of the design, providing a higher degree of customization and security in photonic PUF applications. During the testing process, the temperature of all devices was regulated using a temperature-controlled chip stage, maintaining a constant 25°C. While we controlled the temperature to ensure consistent and reliable measurements, it's important to note that temperature variations could also serve as an additional factor in generating unique responses for PUFs. However, this aspect was not explored in the current study.

Authentication system

To ensure the integrity and security of our PUF devices, we have developed an authentication system similar to[11] that authorizes access only to verified identities. This system utilizes challenge-response pairs (CRPs), capitalizing on the unique properties of the tokens derived from CDCs. The aim is to authenticate legitimate users and prevent unauthorized access. The operational framework of this authentication system is illustrated in Fig. 6a.

The system involves a multi-wavelength laser whose output is modulated by a Mach–Zehnder Modulator (MZM), generating a challenge that combines two elements: time and wavelength. This dual-factor challenge, as shown in Fig. 6a, adds diversity and complexity, enhancing security. The challenge signal passes through the token, and the response is captured and then digitized by an Analog-to-Digital Converter (ADC). This digital response, when paired with the initial challenge, forms a CRP that is crucial for authenticating legitimate users. In our design, the ADC employs 3-bit quantization to convert the response of the token into digital signals.

An illustrative example of an authentication scenario is shown in Fig. 6b, where both a duplicated (adversary) and a legitimate PUF token are evaluated. The system differentiates between the adversary's token and the legitimate user's PUF by analyzing their responses to a set of challenges, thereby ensuring secure access. We modeled this authentication system using the transmission data collected from each device, demonstrating

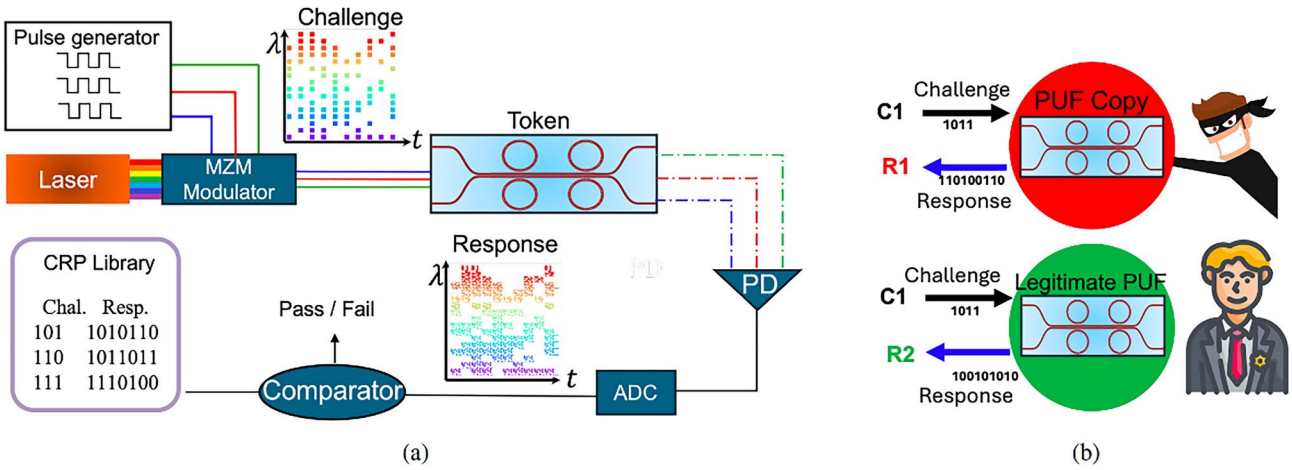

Fig. 6. (**a**) Authentication system demonstration (**b**) Authentication scenario where two different copy and legitimate PUF are used to access the system.

its theoretical viability. The experimental implementation of this authentication setup remains a focus for our future work.

Response evaluation

Upon receiving a challenge, the PUF device generates a response based on its inherent physical characteristics. This response is evaluated using a comparator, which assesses it against the expected response stored in a CRP library. This library, created using the legitimate PUF device, contains a database of valid challenge-response pairs. If the response from the PUF device matches the expected response in the CRP library, the authentication is considered successful, granting access to the user or system. Conversely, if the response deviates from the expected response, indicating an unauthorized attempt or tampering, the authentication fails, and access is denied.

To evaluate the responses, we utilize the fractional Hamming distance. The fractional Hamming distance (FHD) can be viewed as the probability that a bit in one sequence differs from the corresponding bit in another sequence. FHD can be described as:

$$\mathrm{FHD} = \frac{1}{n}\sum_{i=1}^{n}(a_i \oplus b_i) \tag{3}$$

where a_i and b_i are the bits at the $i\mathrm{th}$ position in the two binary sequences, respectively, and $\oplus$ denotes the XOR operation. The value of FHD ranges from 0 to 1, where an FHD of 0 indicates that the two sequences are identical, and an FHD of 1 means that the two sequences are completely different (i.e., complementary). In the context of PUFs, a fractional Hamming distance close to 0.5 is desirable, as it suggests that the responses generated by different devices are sufficiently random and uncorrelated. Because the average FHD between the two long random binary sequences is 0.5. This randomness is crucial for ensuring the security and unpredictability of the PUF, as it minimizes the risk of predictability or cloning by an adversary.

For the intra-hamming distance, we measure the consistency of a specific PUF's response to the same challenge across multiple interrogations. This metric is widely accepted in the hardware security community and has been extensively used in other state-of-the-art works[2,11,15,33] to evaluate the robustness and reliability of PUF designs. By ensuring a low intra-Hamming distance, we can confirm the repeatability and stability of the PUF's response, which is crucial for reliable identification and authentication.

The inter-hamming distance ($\mathrm{HD}_{\mathrm{inter}}$) between the binary response of any two different devices for the same PUF design with a challenge vector $\mathrm{Ch} = \{\mathrm{Ch}_1, \mathrm{Ch}_2, \ldots, \mathrm{Ch}_m\}$ embedded in it can be expressed as:

$$\mathrm{HD}_{\mathrm{inter}} = P(R_i(\mathrm{Ch}) \neq R_j(\mathrm{Ch})) \tag{4}$$

where $R_i(\mathrm{Ch})$ and $R_j(\mathrm{Ch})$ represent the responses of the *ith* and *jth* devices, respectively, for a given challenge vector. For $\mathrm{HD}_{\mathrm{inter}}$ we calculate the responses of multiple copies of the same PUF, fabricated on the same chip, to the same challenge.

Similarly, the intra-fractional Hamming distance can be expressed as:

$$\mathrm{HD}_{\mathrm{intra}} = P(R_i(\mathrm{Ch}_1) \neq R_i'(\mathrm{Ch}_2)) \tag{5}$$

where $R_i(\mathrm{Ch}_1)$ and $R_i'(\mathrm{Ch}_2)$ are the responses of the *ith* device to the two challenges Ch_1 and Ch_2, respectively. For $\mathrm{HD}_{\mathrm{intra}}$ we calculate the responses of multiple challenges of a specific chip. The Hamming distance evaluation results are shown in Fig. 7a and b. Our analysis shows a high inter-Hamming distance between different copies of the PUF, even though multiple copies of the same PUF were fabricated on the same chip and analyzed under the same challenge. The inter-Hamming distance could be further improved by using PUFs fabricated on different chips and in different fabrication facilities, which would introduce greater variability and further enhance the uniqueness of each PUF. For calculating the intra-hamming distance, we conducted two different data acquisitions from our PUF, spaced 11 days apart. We consistently observed a low intra-Hamming distance, demonstrating high repeatability. Utilizing fiber-attached coupling could further enhance this repeatability by

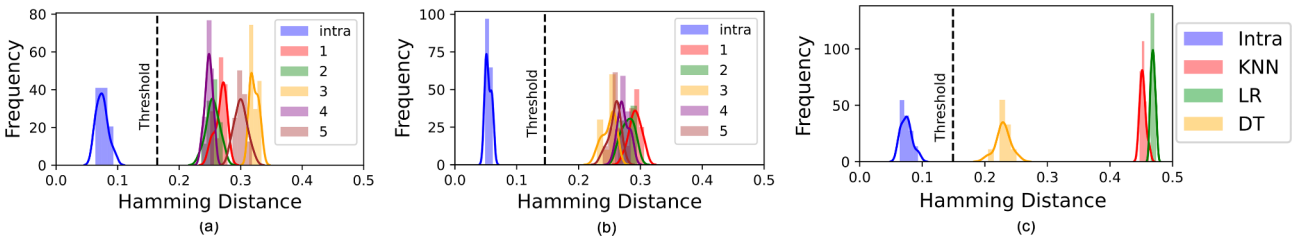

Fig. 7. Intra- and inter-device hamming distance. (**a**) Randomly apodized CDC with five variations. (**b**) P-MRR-assisted P-CDC with five variations. (**c**) ML digital copy hamming distance on randomly apodized CDC device.

preventing misalignment issues with the fiber array-key factors that contribute to a higher intra-Hamming distance. The combination of a high inter-Hamming distance and a low intra-Hamming distance creates a clear separation between the two, allowing us to define a reliable threshold boundary for secure identification and authentication.

Based on our modeling, we have established a decision threshold to differentiate between legitimate devices and their copies. The decision threshold is defined to optimize the separation between legitimate and adversarial devices in terms of Hamming distance and provide a clear boundary between them, enhancing the reliability of PUFs. Therefore the decision point of device *DP* is

$$DP = \frac{\max(\mathrm{HD}_{\mathrm{intra}}) + \min(\mathrm{HD}_{\mathrm{inter}})}{2} \tag{6}$$

$\max(\mathrm{HD}_{\mathrm{intra}})$ is the maximum intra-Hamming distance, representing the worst-case Hamming distance within the same device and, $\min(\mathrm{HD}_{\mathrm{inter}})$ is the minimum inter-Hamming distance, representing the worst-case Hamming distance between different devices. This decision threshold balances the worst-case scenarios from both intra- and inter-hamming distances, aiming to improve the distinctiveness and security of PUF-based systems. By setting the threshold at the midpoint between these two extremes, the design ensures that there is a sufficient margin to distinguish legitimate device responses from adversarial ones, thereby validating the effectiveness of the devices as PUFs. The decision threshold is chosen to balance noise tolerance for authorized authentication while maintaining a strong boundary against unauthorized access, thereby enhancing security. The threshold selection for a PUF depends on the application's noise environment. In noisy conditions, a threshold near the inter-Hamming distance improves noise resilience. Conversely, in a low-noise condition, prioritizing security by selecting a threshold closer to the intra-Hamming distance would be advisable.

Figure 7a and b illustrate the distributions of these Hamming distances, demonstrating a clear boundary that supports the use of these devices as PUFs. This visual representation underscores the effectiveness of the chosen decision threshold in providing a robust security measure. These results are based on testing two devices, for which we had multiple copies, ensuring reliable calculations. All these devices were fabricated in the same batch and are physically proximate, yet significant differences were observed in the keys generated from the same copies. These discrepancies could be more pronounced if the devices are fabricated through different foundries or on a larger scale, as the fabrication process variability patterns differ across chips, wafers, runs, and foundries.

Evaluation of PUF security under machine learning attacks

Here, we evaluate the security of our proposed PUF by subjecting it to machine learning (ML) attacks. We trained three different ML models on a random dataset consisting of 10,000 challenge-response pairs (CRPs) generated by the base device. The trained models were then tested on 10 previously unseen challenges to assess their predictive capabilities. The performance of the ML attacks was measured using the Hamming distance between the predicted responses and the actual PUF responses. The results are shown in Fig. 7c.

For our experiments, we utilized three machine learning models: K-Nearest Neighbors (KNN)[17], Logistic Regression (LR)[18,34], and Decision Tree (DT)[19]. KNN is a simple, yet powerful non-parametric algorithm used for classification and regression. It is particularly effective at capturing local structures in data, making it suitable for testing the ability of our PUF to resist attacks based on close proximity patterns in the CRPs. LR is a widely used statistical model for binary classification problems. It is useful in understanding the relationship between the challenge (input) and response (output). LR tests the PUF's resilience against linear models that might try to find a direct mapping between challenges and responses. DT algorithms are versatile tools capable of handling non-linear data and capturing complex decision boundaries. They are effective in evaluating the PUF's resistance to structured attack models that attempt to exploit hierarchical relationships in the CRPs.

From the results, we observe that none of the ML models were able to predict responses close to the actual PUF responses. The average Hamming distances for the models are as follows. The DT model demonstrated superior performance compared to the other models, likely due to its ability to more effectively capture and learn the patterns within the data. However, despite this enhanced performance, there remains a significant gap between the Hamming distance achieved by the DT model and the intra-device Hamming distance, indicating that the DT model is still far from perfectly mimicking the device's responses. These high Hamming distances indicate a significant dissimilarity between the predicted and actual responses.

The high Hamming distances obtained across all tested models demonstrate the resilience of our PUF against ML attacks. Specifically, the KNN and LR models are unable to capture the inherent complexity of the PUF's response pattern, as evidenced by their high Hamming distance. These results suggest that our PUF design possesses a high level of unpredictability and complexity, effectively thwarting attempts by ML models to accurately predict the responses based on the given challenges.

All CRPs used for training correspond to the same token and noise-free, ensuring a large and representative training set. This approach was chosen to represent a worst-case scenario for a machine learning (ML) attack, demonstrating that our PUF can withstand such challenges. As illustrated in Fig. 6a and aligned with state-of-the-art designs[11], a CRP includes a series of wavelengths transmitted over a time series, making the system a robust pair of CRPs. In our system, t, the number of samples sent sequentially during an authentication trial, is 32. Each CRP contains 32 samples, with each sample being 30 bits in size, derived from 10 wavelengths quantized to 3 bits per wavelength. While reducing t could potentially increase the authentication speed, it would weaken the PUF.

However, we do not favor reducing the number of samples (t) since our PUF can operate at an extremely high frequency, and time is not a significant constraint in our design.

Conclusion

In this study, we have developed and experimentally evaluated advanced Silicon PUFs using CDC structures. Our research introduces several innovative design enhancements, including perforated configurations and MRR integrations, to significantly increase the complexity and unpredictability of these devices. We demonstrated that even minor variations in the hole distribution and grating periods can profoundly affect the spectral responses of CDCs. These variations are crucial for generating unique and unclonable responses that form the basis of robust PUFs. Our results highlight the sensitivity of CDCs to FPVs, which is a key feature for PUFs as it ensures that each device has a distinct and secure response.

We tested these designs against three different machine learning attacks, achieving a Hamming distance of over 0.4 with a standard deviation of less than 0.01 at a quantization level of three, using 10,000 samples of challenge-response pairs. These results underscore the potential of silicon photonic PUFs in optical communication systems, showing the advantages of using CDC-based PUFs for secure authentication and anti-counterfeiting applications. By harnessing the intrinsic manufacturing variations and intricate design features of SiPh, we can create highly secure, unclonable devices suitable for deployment in sensitive and high-risk environments.

Methods

In this study, we analyzed over 200 devices, including both identical copies and various designs, strategically distributed across a 10×10 mm chip. The chip was fabricated using the standard electron beam (E-Beam) multi-project wafer (MPW) process at Applied Nanotools Inc[27], with a standard 220-nm silicon-on-insulator (SOI) platform. The sporadic placement allowed each design to experience different FPVs due to their differing positions on the chip.

We conducted testing using an automated station from Maple Leaf Photonics[35], capable of handling single dies up to 25×25 mm in size. The test setup comprised four main components: a laser source, a polarization controller set to TE mode, a fiber array attached to the station, and a photodetector. The chip was fixed on a stage, while the fiber arm provided automated movement in the X, Y, Z, yaw, and pitch directions. These movements were crucial for achieving precise alignment of the fiber array with the chip, enabling low-loss measurements. To maintain optimal testing conditions, the temperature of the chip was regulated using a temperature controller, which kept the chip at a constant 25°C throughout the testing process. This precise temperature control was essential for ensuring consistent and accurate measurements by preventing thermal fluctuations from affecting the device's performance. To further minimize environmental disturbances, the setup was placed on a floating table, and a manual polarization controller was positioned between the laser and the device under test (DUT) to ensure consistent polarization. However, surrounding disturbances and different alignments of the test setup can introduce minor disturbances. These factors likely contributed to the small variations observed between the two tests.

Coupling to the grating couplers (GCs) on the chip was facilitated by a single-mode fiber array with a 127-μm pitch. For accurate alignment between the chip and the fiber array, we used two digital microscopic cameras integrated into the testing station. The laser source, an Agilent HP 8164A, operated within the C-band, covering a wavelength range from 1460 nm to 1580 nm with a fine resolution of 0.1 pm. Light detection from the chip was performed using the Keysight 81635A dual optical photodetector, which operates across a wavelength range from 800 nm to 1650 nm and a power spectrum range from $+10$ to -80 dBm. Single-mode fibers were used for all connections within the setup to ensure high precision and minimal loss.

The input power was set to 7.5 dBm, resulting in a total output loss of 25.2 dB. This loss included 17.6 dB from the grating couplers (8.8 dB each) and approximately 1 dB per device. Consequently, the total unaccounted losses due to the test setup and alignment were approximately 6.6 dB.

Data availibility

The datasets generated and/or analyzed during the current study are not publicly available due to pending patent applications and the proprietary nature of the data. However, they are available from the corresponding author upon reasonable request.

Received: 30 June 2024; Accepted: 11 September 2024
Published online: 26 October 2024

References

1. Gao, Y., Al-Sarawi, S. F. & Abbott, D. Physical unclonable functions. *Nat. Electron.* **3**, 81–91. https://doi.org/10.1038/s41928-020-0372-5 (2020).
2. Goki, P. N. *et al.* Optical identification using physical unclonable functions. *J. Opt. Commun. Netw.* **15**, E63–E73. https://doi.org/10.1364/JOCN.489889 (2023).
3. Nadimi Goki, P., Mulugeta, T. T., Caldelli, R. & Potì, L. Optical systems identification through rayleigh backscattering. *Sensors* **23**, 5269 (2023).
4. Gatti, U. One-time programmable memories for harsh environments. In *Rad-hard Semiconductor Memories*, 151–189 (River Publishers, 2022).
5. Cratere, A., Gagliardi, L., Sanca, G. A., Golmar, F. & Dell'Olio, F. State-of-the-art and future trends, On-board computer for cubesats. *IEEE Access* (2024).
6. Herder, C., Yu, M.-D., Koushanfar, F. & Devadas, S. Physical unclonable functions and applications: A tutorial. *Proc. IEEE* **102**, 1126–1141. https://doi.org/10.1109/JPROC.2014.2320516 (2014).

7. Pavanello, F., O'Connor, I., Rührmair, U., Foster, A. C. & Syvridis, D. Recent advances in photonic physical unclonable functions. In *2021 IEEE European Test Symposium (ETS)* 1–10. https://doi.org/10.1109/ETS50041.2021.9465434 (IEEE, 2021).
8. Surendranathan, U. *et al.* Total ionizing dose effects on the power-up state of static random-access memory. *IEEE Trans. Nucl. Sci.* **70**, 641–649. https://doi.org/10.1109/TNS.2023.3236625 (2023).
9. Du, Q. *et al.* Gamma radiation effects in amorphous silicon and silicon nitride photonic devices. *Opt. Lett.* **42**, 587–590. https://doi.org/10.1364/OL.42.000587 (2017).
10. Boynton, N. *et al.* Gamma radiation effects on passive silicon photonic waveguides using phase sensitive methods. *Opt. Express* **28**, 35192–35202. https://doi.org/10.1364/OE.401299 (2020).
11. Grubel, B. C. *et al.* Silicon photonic physical unclonable function. *Opt. Express* **25**, 12710–12721. https://doi.org/10.1364/OE.25.012710 (2017).
12. Smith, A. M. & Jacinto, H. S. Reconfigurable integrated optical interferometer network-based physically unclonable function. *J. Lightwave Technol.* **38**, 4599–4606. https://doi.org/10.1109/JLT.2020.2996015 (2020).
13. Jacinto, H. S., Smith, A. M. & Rafla, N. I. Utilizing a fully optical and reconfigurable puf as a quantum authentication mechanism. *OSA Continuum* **4**, 739–747. https://doi.org/10.1364/OSAC.399294 (2021).
14. Jimenez, P. *et al.* Photonic physical unclonable function based on symmetric microring resonator arrays. *Fron. Opt.*. https://doi.org/10.1364/FIO.2023.JTu4A.82 (2023).
15. Tarik, F. B., Famili, A., Lao, Y. & Ryckman, J. D. Scalable and cmos compatible silicon photonic physical unclonable functions for supply chain assurance. *Sci. Rep.* **12**, 15653. https://doi.org/10.1038/s41598-022-19796-z (2022).
16. Mahdian, M. A., Taheri, E., Mojaver, K. H. R. & Nikdast, M. Photonic physically unclonable functions using ring-assisted contra-directional couplers. In *Optical Fiber Communication Conference* W2A–22 (Optica Publishing Group, 2024).
17. Viana, C. B., Araújo, C. J. & de Araújo, D. R. Identifying physical unclonable functions using classifier algorithms. In *2023 IEEE Latin American Conference on Computational Intelligence (LA-CCI)* 1–5 (IEEE, 2023).
18. Rührmair, U. *et al.* Puf modeling attacks on simulated and silicon data. *IEEE Trans. Inf. Forensics Secur.* **8**, 1876–1891 (2013).
19. Shah, N., Chatterjee, D., Sapui, B., Mukhopadhyay, D. & Basu, A. Introducing recurrence in strong pufs for enhanced machine learning attack resistance. *IEEE J. Emerg. Select. Topics Circ. Syst.* **11**, 319–332 (2021).
20. Shi, W. *et al.* Silicon photonic grating-assisted, contra-directional couplers. *Opt. Express* **21**, 3633–3650. https://doi.org/10.1364/OE.21.003633 (2013).
21. Lin, S. *et al.* Computational lithography for silicon photonics design. *IEEE J. Sel. Top. Quantum Electron.* **26**, 1–8. https://doi.org/10.1109/JSTQE.2019.2958931 (2019).
22. Hammood, M. *et al.* Broadband, silicon photonic, optical add-drop filters with 3 db bandwidths up to 11 thz. *Opt. Lett.* **46**, 2738–2741. https://doi.org/10.1364/OL.423745 (2021).
23. Qiu, H. *et al.* Narrow-band add-drop filter based on phase-modulated grating-assisted contra-directional couplers. *J. Lightwave Technol.* **36**, 3760–3764. https://doi.org/10.1109/JLT.2018.2852483 (2018).
24. Tunesi, L. *et al.* Thermal control scheme in contra-directional couplers for centered tunable bandwidths. In *2023 International Conference on Numerical Simulation of Optoelectronic Devices (NUSOD)* 115–116. https://doi.org/10.1109/NUSOD59562.2023.10273529 (IEEE, 2023).
25. Boroojerdi, M., Ménard, M. & Kirk, A. Two-period contra-directional grating assisted coupler. *Opt. Express* **24**, 22865–22874. https://doi.org/10.1364/OE.24.022865 (2016).
26. Mahdian, M. A., Tunesi, L., Bardella, P. & Nikdast, M. Bandwidth-adaptive single-and double-channel silicon photonic contra-directional couplers. In *2023 IEEE Photonics Conference (IPC)* 1–2. https://doi.org/10.1109/IPC57732.2023.10360616 (IEEE, 2023).
27. Applied Nano Technologies. Applied nano technologies. https://www.appliednt.com/. Accessed 03 June 2024.
28. Gostimirovic, D., Xu, D.-X., Liboiron-Ladouceur, O. & Grinberg, Y. Deep learning-based prediction of fabrication-process-induced structural variations in nanophotonic devices. *ACS Photonics* **9**, 2623–2633. https://doi.org/10.1021/acsphotonics.1c01973 (2022).
29. Cauchon, J., St-Yves, J. & Shi, W. Thermally chirped contra-directional couplers for residueless, bandwidth-tunable bragg filters with fabrication error compensation. *Opt. Lett.* **46**, 532–535 (2021).
30. Shiran, H., Mojaver, H. R., Bachman, J., Jin, C. & Liboiron-Ladouceur, O. Impact of sio 2 cladding voids in siph building blocks. In *2020 IEEE Photonics Conference (IPC)* 1–2. https://doi.org/10.1109/IPC47351.2020.9252413 (IEEE, 2020).
31. Mirza, A. *et al.* Silicon photonic microring resonators: A comprehensive design-space exploration and optimization under fabrication-process variations. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.* **41**, 3359–3372. https://doi.org/10.1109/TCAD.2021.3132555 (2021).
32. Chen, A., Begović, A., Anderson, S. & Huang, Z. R. On-chip slow-light sin bragg grating waveguides. *IEEE Photonics J.* **14**, 1–6 (2022).
33. Civelli, S., Goki, P. N., Parente, E., Potì, L. & Secondini, M. Optical identification for user authentication in quantum key distribution systems. In *49th European Conference on Optical Communications (ECOC 2023)*, vol. 2023, 815–818 (IET, 2023).
34. Bishop, C. M. & Nasrabadi, N. M. *Pattern recognition and machine learning* Vol. 4 (Springer, 2006).
35. Maple Leaf Photonics. Maple leaf photonics. https://www.mapleleafphotonics.com/. Accessed 03 June 2024.

Acknowledgements

The authors would like to express their gratitude to Asif Mirza and Lorenzo Tunesi for their invaluable assistance, which was crucial in making this work possible. This research was supported by the National Science Foundation (NSF) under grants CNS-2046226 and CCF-2006788.

Author contributions

M.A.M. was responsible for all device-level simulations, layout design, and testing of the fabricated devices. E.T. utilized the test results to perform Hamming distance analysis and develop the machine learning models. K.R.M. provided crucial guidance on conducting the tests and modeling the authentication system. M.N. led and advised the team in performing the tests and analyses conducted in this work. All authors analyzed and discussed the results. All authors contributed to writing and reviewing the manuscript.

Declarations

Competing interests

The authors are pursuing a patent application, related to this work, with the U.S. Patent and Trademark Office.

Additional information

Correspondence and requests for materials should be addressed to M.N.