



## ISTITUTO NAZIONALE DI RICERCA METROLOGICA Repository Istituzionale

Quantifying the Sensitivity and Unclonability of Optical Physical Unclonable Functions

*Original*

Quantifying the Sensitivity and Unclonability of Optical Physical Unclonable Functions / Emanuele Lio, Giuseppe; Nocentini, Sara; Pattelli, Lorenzo; Cara, Eleonora; Wiersma, DIEDERIK SYBOLT; R??hrmair, Ulrich; Riboli, Francesco. - In: ADVANCED PHOTONICS RESEARCH. - ISSN 2699-9293. - 4:2(2022), p. 2200225. [10.1002/adpr.202200225]

*Availability:*

This version is available at: 11696/75879 since: 2023-03-01T11:57:07Z

*Publisher:*

Wiley

*Published*

DOI:10.1002/adpr.202200225

*Terms of use:*

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

*Publisher copyright*

WILEY

This article may be used for non-commercial purposes in accordance with Wiley Terms and Conditions for Use of Self-Archived Versions

(Article begins on next page)

# Quantifying the Sensitivity and Unclonability of Optical Physical Unclonable Functions

Giuseppe Emanuele Lio,\* Sara Nocentini, Lorenzo Pattelli, Eleonora Cara, Diederik Sybolt Wiersma, Ulrich Rührmair, and Francesco Riboli\*

Due to their unmatched entropy, complexity, and security level, optical physical unclonable functions (PUFs) currently receive a lot of interest in the literature. Despite the large body of existing works, herein, one of their core features in detail is studied, namely, their physical unclonability. This article tackles this fundamental and yet largely unaddressed issue. In simulations and/or experiments, the sensitivity of diffraction-based optical responses is investigated with respect to various small alterations such as variation in position, size, and number of the scatterers, as well as perturbations in the spatial alignment between the PUF and the measurement apparatus. The analysis focuses on 2D optical PUFs because of their relevance in integrated applications and the need to reply to security concerns that can be raised when the physical structure of the geometry is accessible. Among the results of this study, the sensitivity analysis shows that a positional perturbation of scatterers on the order of 30 nm, that is, far below the wavelength of the probing laser light of 632 nm wavelength, is sufficient to invalidate the PUF response and thus detect forgery attempt. These results support and quantify the high adversarial efforts required to clone optical PUFs, even for 2D layouts.

techniques to this end rely on the permanent storage of digital secret keys in electronic devices, for example, in smartphones, car keys, bank cards, passports, or computers. Unfortunately, the last decades have seen an explosion of attacks that can extract such keys unnoticed, including sophisticated malware and physical methods.<sup>[2–4]</sup> This obviously calls for new authentication approaches with improved security features.

The use of nondigital primitives such as physical unclonable functions (PUFs) constitutes a promising new avenue in this context.<sup>[5–8]</sup> PUFs are randomly structured physical systems which exhibit a complex input–output or, in PUF parlance, “challenge–response” behavior that is unique to each PUF. Their uncontrollable individual disorder on small length scales makes them practically unclonable, even for their original manufacturer. Due to their physical nature, randomness, and unclon-


ability, PUFs can disable various popular attack vectors compared to classical, permanently stored keys: For example, their physical nature obviously prevents that PUFs are stolen remotely over a purely digital data connection by attackers.<sup>[2,9]</sup> As another example, PUFs allow the short-term derivation of individual secret key material in devices, avoiding the long-term and attack-prone presence of secrets in digital memory. This usually complicates key extraction<sup>[2]</sup> and side channel attacks.<sup>[9]</sup> Finally, some special,

## 1. Introduction

According to recent estimates,<sup>[1]</sup> the looming internet of things and worldwide information exchange by the year 2018–2023 will produce a global data stream of around tens zettabytes per annum. This requires secure and reliable authentication methods in order to protect private information and to safeguard access to personal devices and services. The currently widespread

G. E. Lio, F. Riboli  
Nation Institute of Optics  
National Research Council (CNR-INO)  
Via Nello Carrara 1, 50019 Sesto Fiorentino, Florence, Italy  
E-mail: giuseppeemanuele.lio@unifi.it; riboli@lens.unifi.it

G. E. Lio, S. Nocentini, L. Pattelli, D. S. Wiersma, F. Riboli  
European Laboratory for Non-Linear Spectroscopy (LENS)  
University of Florence  
Via Nello Carrara 1, 50019 Sesto Fiorentino, Florence, Italy

 The ORCID identification number(s) for the author(s) of this article can be found under <https://doi.org/10.1002/adpr.202200225>.

© 2022 The Authors. Advanced Photonics Research published by Wiley-VCH GmbH. This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

DOI: 10.1002/adpr.202200225

G. E. Lio, D. S. Wiersma  
Physics Department  
University of Florence  
Via Sansone, 1, 50019 Sesto Fiorentino, Florence, Italy

S. Nocentini, L. Pattelli, E. Cara, D. S. Wiersma  
Advanced Materials Metrology & Life Sciences  
Istituto Nazionale di Ricerca Metrologica (INRiM)  
Strada delle Cacce 91, Turin 10135, Italy

U. Rührmair  
Physics Department  
LMU München  
Schellingstraße 4/III, D-80799 München, Germany

U. Rührmair  
Electrical and Computer Engineering (ECE) Department  
University of Connecticut  
Storrs 06269, CT, USA

advanced subclasses of PUFs can remain practically unclonable and thus secure even if all their internal disorder and structure is known, simply due to the current limits of nanofabrication.<sup>[5,10]</sup> This makes these special PUFs innately immune against any key-extracting and even any secret-extracting attacks, a seminal property sometimes referred to as “secret-freeness”.<sup>[10]</sup>

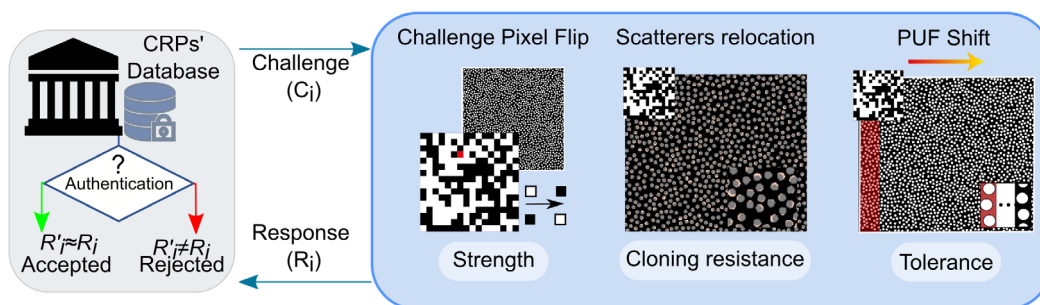
Within the ample research landscape of magnetic,<sup>[11]</sup> silicon<sup>[6,12–15]</sup> or radiowave-based<sup>[16]</sup> PUFs, optical and photonic versions have played a pivotal role since their first proposal in 2002<sup>[5]</sup> and subsequently implemented in a quantum read-out scheme.<sup>[17,18]</sup> A generic optical physical unclonable function consists typically of a scattering material, which generates a complex light diffraction pattern when illuminated with coherent light, providing a particularly sensitive and convenient probing mechanism for such systems.<sup>[5,19–22]</sup> Laser light can resolve their unique structures with subwavelength sensitivity, leading to strong security levels and high resilience against cloning.<sup>[5,19–21,23]</sup> By using passive or active materials of different nature (integrated light sources in dielectric or metallic systems), and by playing with the systems’ dimensionality (2D or 3D), a large variety of optical PUFs can be conceived, as research in the last decades has demonstrated. This includes PUFs based on organic nanoemitters,<sup>[24–26]</sup> chip-scale laser,<sup>[27]</sup> thin random scattering layers of plasmonic nanoparticles,<sup>[28–31]</sup> random silver nanostructures,<sup>[32,33]</sup> or even PUF architecture compatible with microfabrication technologies for photonic integrated circuits (PIC).<sup>[34–37]</sup> In the end, any material with random structure, defects, or scattering elements, including regular paper,<sup>[38]</sup> will generate complex speckle patterns when illuminated by a coherent source, making optical PUFs a highly efficient, inexpensive, and robust platform for secure authentication.<sup>[5,8,32,39,40]</sup> In recent years, 2D optical PUFs have attracted particular attention due to their high stability, industry-compatible fabrication processes and straightforward integration with existing telecommunication technologies.<sup>[34–36]</sup> At the same time, however, these 2D structures inevitably exhibit a lower complexity and entropy than comparable 3D systems. They also can be directly inspected by electron microscopy or other diagnostic techniques and are therefore easier—at least in principle—to replicate or “clone,” both experimentally and numerically in simulations. For these reasons, in view of their future widespread adoption, an accurate estimate of their cryptographic security is fundamental and in this work, we quantitatively evaluate their resilience to cloning attacks and sensitivity to measurement

perturbations. In more detail, the experimental and numerical analysis carried out in this work quantifies the sensitivity and the unclonability of a prototypical 2D optical PUF by comparing the keys generated by different clones of the same primitive or studying the keys variation to small readout alterations. Perturbations considered include the imperfect cloning of the PUF layout (e.g., due to slightly incorrect number, position, or alignment of the scattering elements), as well as errors during the illumination or readout process. All results are interpreted under a unified framework, which allows us to cast a direct connection between the experimental device and its simulated counterpart. Moreover, the results obtained from the analysis of 2D PUFs are also relevant to more complex 3D architectures, as they can be considered as a lower bound to evaluate unclonability, stability, and other properties in 3D PUFs. Please recall in this context that with current computational methods, exact simulations of 3D optical PUFs are extremely demanding and time-consuming compared to the 2D case.

## 2. Background and Methodology

### 2.1. Use Case: Remote Identification

The typical use case for so-called optical Strong PUFs<sup>[41]</sup> consists of a remote identification protocol, in which a PUF (or a user holding it) identifies remotely via a digital communication channel to a central authority. The protocol employs a large number of input–output pairs or challenge–response pairs (CRPs) of the PUF as a unique identifier or “fingerprint” and is sketched in **Figure 1**. As a preparatory initial step, we assume that the central authority has measured a sufficiently large database of CRPs for the PUF. We also assume the authority has determined some error-tolerating threshold value to ensure a successful identification of the PUF in variable and error-prone everyday conditions. The threshold must be set in such a way to allow discriminating between the responses of original PUFs and perturbed responses generated by possible read-out errors (challenge pixel flip), nonperfect clones of the original PUF (scatterers relocation), or slight misalignment between the original PUF and the read-out system (PUF misalignment); see Figure 1. Once these setup steps have been accomplished, the PUF is handed over from the authority to the user. During the authentication phase or identification protocol, the authority sends a series of randomly chosen challenges from its database to the



**Figure 1.** a) Schematic representation of the authentication flowchart based on optical PUFs. Potential attack scenarios or issues with this scheme include: 1) the challenges  $C_i$  are affected by noise (single or multiple macro-pixel flip); 2) the optical PUF scatterers are misplaced (small structural perturbations or cloning imperfections); and 3) the optical PUF is misaligned with respect to the illumination/readout system.

PUF/user and awaits the correct responses in return. Once they arrive, the incoming responses are compared to the responses measured earlier in the preparatory phase by the authority. If they match within the predefined error threshold (see above), then the identity of the PUF/user is confirmed. We stress that each CRP can be used only once in the above protocol. This means that the pre-established CRP list shrinks over time and must be planned large enough in the setup phase for the entire application lifetime.

## 2.2. Experimental Setup

To experimentally address these cases, we built an optical setup able to generate the CRPs and authenticate each entity, following the scheme sketched in **Figure 2a**. It comprises a He–Ne laser ( $\lambda = 633$  nm), a digital micromirror device (DMD) for the challenge manipulation, illumination and collection optics, and a CCD camera to record the responses. Additional details about the experimental apparatus are reported in the Experimental Section and in Figure S1, Supporting Information. The 2D optical PUF consists of a perforated metallic membrane obtained starting from a disordered 2D arrangement of polystyrene nanospheres (see insets of Figure 2a,b). Additional details are available in the Experimental Section and in Figure S3, Supporting Information. Because of the fabrication method based on an uncontrolled self-assembly process, even the manufacturer cannot replicate the same PUF design twice.

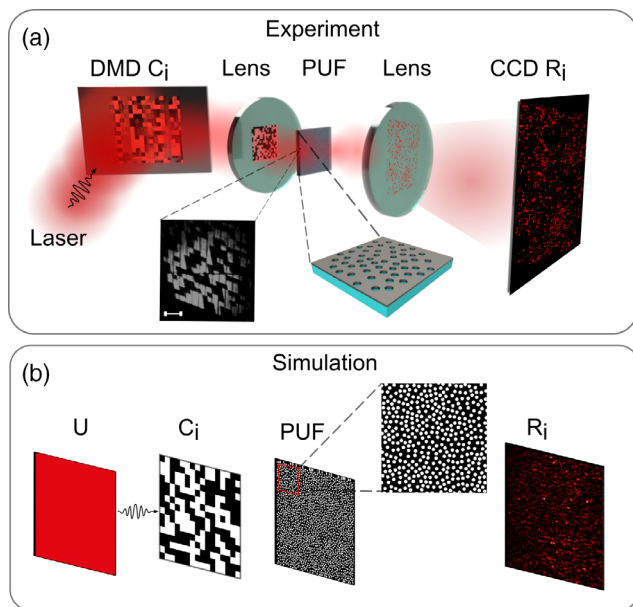
## 2.3. Numerical Simulations

In parallel, the experimental configuration is replicated numerically using an implementation of the Rayleigh–Sommerfeld (RS)

method,<sup>[42–45]</sup> which we have integrated in a routine to generate the sample masks, the challenges, and a speckle registration algorithm. The numerical process consists of four main steps, as depicted in Figure 2b. Numerically, the disordered arrangement of holes in the diffraction mask (i.e., the PUF) is generated by packing nonoverlapping circles using either a random sequential adsorption (RSA) or a Lubachevsky–Stillinger (LS) approach.<sup>[46,47]</sup> These methods are used to pack discs up to a target the packing fraction ( $f_p$ ) defined as the ratio between the area occupied by the disks and the total sample area. Then, a plane wave ( $U$ ) is projected over a pixelated mask to generate the challenge pattern ( $C_i$ ) which is imaged onto the PUF. Following the experimental configuration, the scattered intensity is finally recorded in the far field at an off-axis position on  $XY$  plane at a distance  $z$  from the PUF.

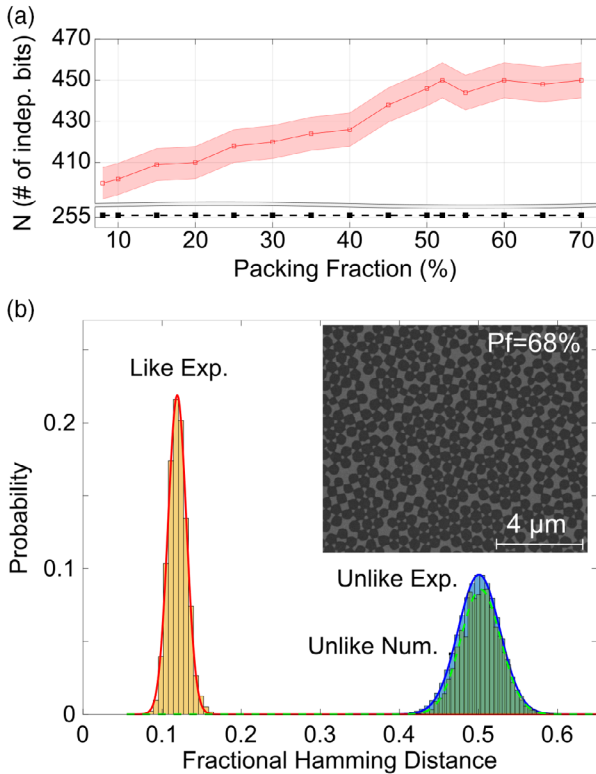
## 2.4. Entropy Estimation for Optical PUFs

To quantify the randomness (entropy or information content), and the stability of the PUF responses against environmental variations, we follow the typical approach used for their application.<sup>[5,48]</sup> The first step is to generate the binary keys ( $K_1, \dots, K_i$  from the responses  $R_1, \dots, R_i$  related to the challenges  $C_1, \dots, C_i$ ) by hashing and reshaping each raw speckle image into a 1D array. This can be performed using standard image transformation and binarization algorithms. Here, the wavelength of a wavelet-based Gabor filter is tuned to extract the features of the speckle images while ensuring the repeatability of the responses under the same challenge interrogation. In general, the process of Gabor hashing and binarization of the response patterns is largely independent on the input laser intensity. The pairwise distance between each binary keys  $K_1, \dots, K_i$  is then measured with the Hamming distance metric.<sup>[48]</sup> Distances between keys generated by different challenges are called “unlike” distances (and are related to the entropy of the key), while those generated by same challenges are called “like” distances (and are related to the stability of the PUF). The entropy of the keys is then evaluated by assuming that each fractional hamming Distance (FHD) resulting from the bit-wise comparison of two different keys can be represented as a Bernoulli trial, albeit with correlations between successive PUF responses. For large  $N$  values, the expected binomial distribution is well approximated by a Gaussian, which makes possible to estimate the number of independent bit of the keys, that is,  $N = \langle p \rangle \cdot (1 - \langle p \rangle) / \sigma^2$ , that is associated with the PUF entropy/information content. Therefore, as a first step, we have generated several synthetic PUF configurations to study how  $N$  depends on  $f_p$  for a fixed subwavelength hole radius  $r_0 \approx 200$  nm. Numerical simulations show that dense perforated masks with  $f_p$  between 50% and 70% generate keys with the highest entropic content; see **Figure 3a**. In addition, we note that the entropy of the key is larger than that of the challenge (composed of  $M \times M$  macropixels), which is  $N_C = \log_2(2)^M$  (see Figure 3a), demonstrating that the interaction between light and the optical PUF effectively increases the information content encoded in the Challenge. The choice of the size of the macropixels is based on the analysis reported in the Challenges pixel size section and in Figure S2, Supporting Information. The optical characterization of the FHD for the experimental PUF



**Figure 2.** a) Sketch of the experimental optical setup used to characterize the proposed optical PUFs. The inset on the left shows the challenges overlapped to the Thorlabs ruler (R1L3S2P) to measure its size (scale bar 100  $\mu$ m) and the inset on the right shows a sketch of the sample. b) Scheme of the numerical workflow used to generate and collect synthetic CRPs.





**Figure 3.** a) Number of independent bits calculated as function of  $f_p$  in synthetic optical PUF samples. b) The blue histogram and solid line correspond to the experimental “unlike” and its fit, the experimental “like” is displayed with the yellow histogram and the red solid line for the fit, while the numerical “unlike” is indicated by the green histogram and its fit by the green dashed line. The inset in b) shows an scanning electron microscope image of the optical PUF, exhibiting a densely packed arrangement of holes etched into a titanium membrane.

sample is reported in Figure 3b, returning a value of  $N = 448$  bits, in excellent agreement with the numerical prediction.

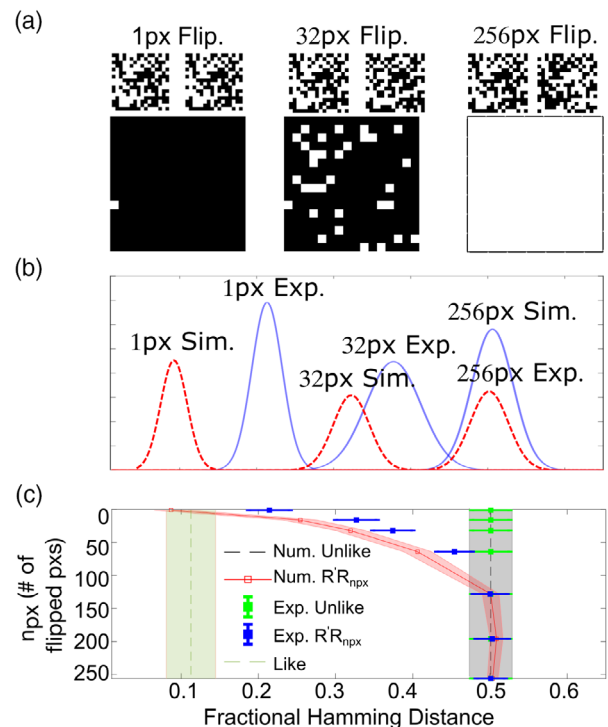
The “like” FHD distribution, which is collected after a time lag of 30 min in order to test the stability and define the acceptance threshold, returns a mean value  $\langle p \rangle$  of 0.122 and a standard deviation  $\sigma = 0.038$  (yellow histogram/red curve in Figure 3b). Since the like and unlike distributions are well separated, the authentication acceptance threshold can be set at around 0.2 to safely reject false positives.<sup>[49]</sup> Due to the deterministic and noiseless nature of numerical calculations, the “like” FHD distribution is not reported here as it would appear as a delta-distribution centered around zero. Based on the good agreement between the FHD histograms and their Gaussian models, in the following, we will plot FHD distributions showing only their fitting curves for better clarity.

## 3. Results and Discussion

### 3.1. Sensitivity to Challenge Pixel Flips

This analysis has been carried out experimentally and verified by numerical calculation. As a first test, we study the sensitivity of

the optical PUF response to perturbations of the challenge (random macropixel flips). We generate a set of 2000 challenges and then perturbed versions of these challenges with one or more random macropixels flipped to its opposite value. An ideal PUF is expected to provide a completely independent response as soon as the challenge is modified, meaning that this test can be used to evaluate the optical PUF sensitivity. Figure 4a shows some illustrative examples of  $16 \times 16$  challenges and their perturbed version, with the flipped pixels drawn in white in the large panels. Figure 4b reports the fit retrieved by the FHD analysis for the experimental and numerical studies. The fits are evaluated on the FHD distributions obtained comparing the responses from the system probed with the original challenges  $R'$  and the responses obtained for the perturbed challenges  $R_{\text{npix}}$ . Figure 4c summarizes the comparison for different degrees of perturbation. Black and green ribbons are shown for reference, representing the experimental “unlike” and “like” FHD distributions, respectively. The numerical and experimental comparison (“interdevice”) FHD distributions of  $R' R_{\text{npix}}$  present a similar trend (red ribbon line and blue dots, respectively). We note that a flip of a few pixels (1–32 pxs) produces  $R' R_{\text{npix}}$  distributions with  $\langle p \rangle$  values ranging from 0.08 (0.23) to 0.35 (0.38) for numerical (experimental) cases, respectively. In the experimental case, even a single pixel flip significantly shifts the  $R' R_{\text{npix}}$  distribution from the “like” one



**Figure 4.** a) Illustrative examples of original and perturbed challenges for different numbers of flipped macropixels. The large panel shows the macropixel that has been flipped. b) Numerical (red) and experimental (blue) “interdevice” FHD distributions for 1, 32, and 256 pixels. c) Trend for numerical and experimental “unlike” (black ribbon line and green dots),  $R' R_{\text{npix}}$  comparison (red ribbon line and blue scatterers), and the experimental “like” (light green ribbon). The error bars are calculated as the standard deviation of each FHD distribution.

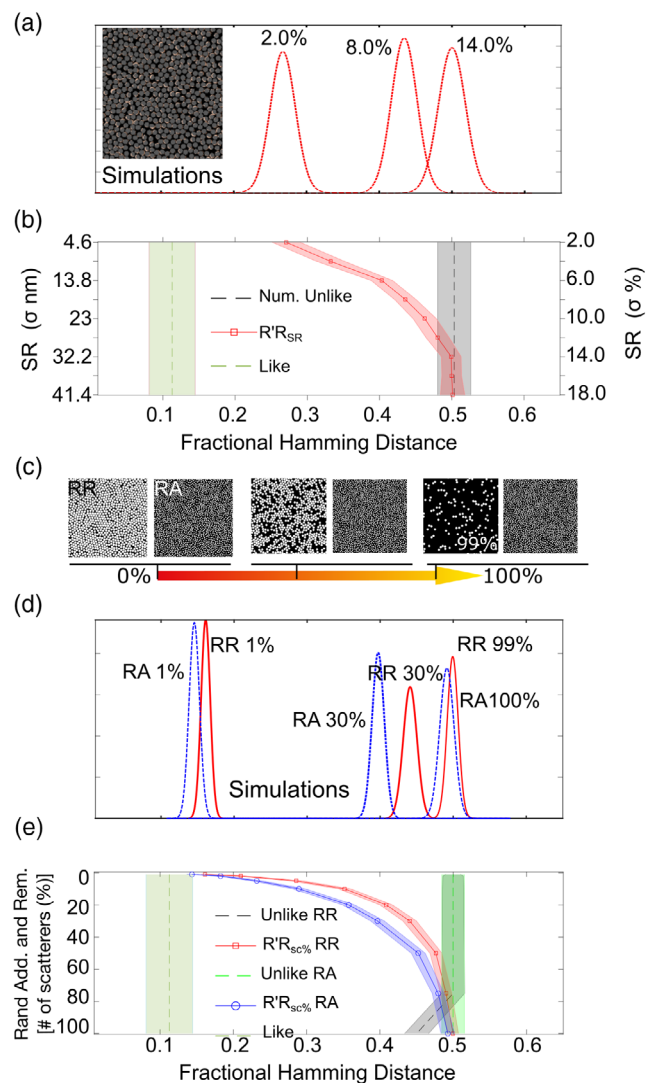
by more than two standard deviations, making the response recognizable from the original response. Flipping an even larger number of pixels ( $>64$  ppx) leads rapidly to FHD distributions with  $\langle p \rangle$  close to 0.5. Despite the bidimensional nature of the sample, the optical PUF shows a good sensitivity to a single-pixel variation of the challenge as the FHD distribution of the responses related to challenges with a single pixel flip are not overlapped with their respective “like” distributions. The effect of the pixel flip perturbation on the speckle pattern is shown in Figure S4, Supporting Information. Given a target illumination area on the PUF device, the number of macropixels in the challenge should be set in a way to maximize the number of available patterns while remaining sensitive to single-pixel flip events. For our experimental configuration, we find that challenges differing by just one macropixel generate responses that are not sufficiently distinguishable (their  $R'_{R_{1px}}$  distribution overlaps with the like distribution) in case of challenges made of  $24 \times 24$  macropixels or more (Figure S5, Supporting Information).

### 3.2. Sensitivity to Scatterers Relocation

The second test that can be addressed numerically concerns the robustness of the PUF to cloning attempts. In this scenario, an attacker trying to clone the physical device aims at replicating the shape, size, and position of all scattering elements. To simulate different degrees of cloning imperfections, we perturb the PUF by adding some Gaussian noise ( $\sigma \approx n_R/r_0$ , where  $n_R$  is the relocation) on the position of each scatterer. The results are summarized in Figure 5a, showing that cloning the holes with a precision  $<5$  nm (below the typical resolution of e-beam lithography fabrications) is already sufficient to relocate the  $R'_{R_{SR\%}}$  FHD distribution at  $\langle p \rangle = 0.25$ , well above the experimental acceptance region. With a precision of about 30 nm, the resulting PUF gives rise to an effectively independent set of responses ( $\langle p \rangle = 0.5$ ), which is remarkable considering that the hole radius  $r_0$  is  $\approx 230$  nm and the probing wavelength is  $\lambda = 633$  nm. A graph that summarizes the behavior for all applied positioning uncertainties is shown in Figure 5b. Further cloning imperfections are represented by two case studies mimicking an increasing modification of the involved scatterers; for this purpose they are randomly removed (RR) or randomly removed and then added again (RA) in new positions, as sketched in Figure 5c. These numerical studies highlight how the “interdevice” (comparison) FHD distributions become independent after RR or RA of  $<20\%$  ( $\langle p \rangle \approx 0.30$ ) well above the experimental acceptance region, as shown in the fits and the summary FHD trend in Figure 5d,e respectively. In order to evaluate the probability of cloning (POC), we calculated the overlap integral of the “like” and the “intra” distributions.<sup>[49–52]</sup> Considering an optimistic case where the clone differs only by 2% from the original one (scatterers relocation, or randomly removed, or removed and added), we estimate POC values that are of the order or smaller than  $10^{-4}$ , see Figure S6, Supporting Information.

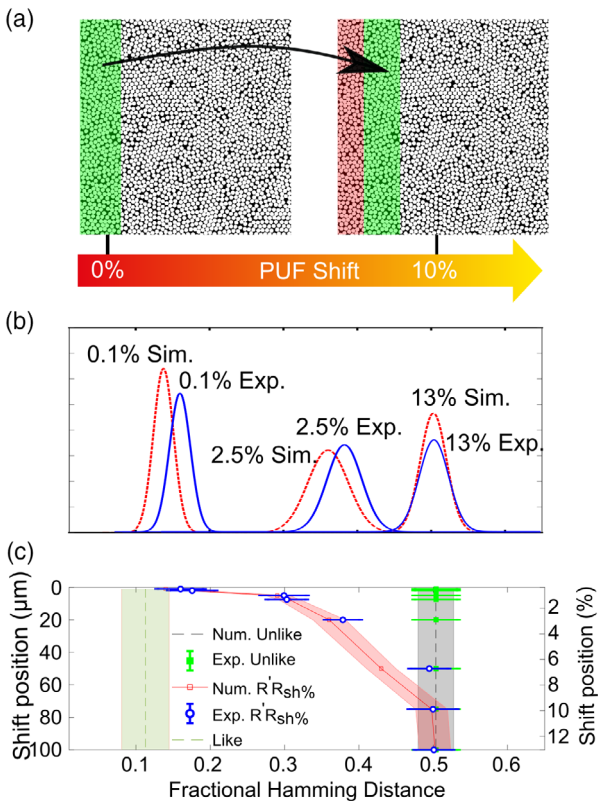
### 3.3. Sensitivity to Misalignment Within Measurement Setup

In this section, we study how the responses are affected by a misalignment of the illuminated region on the optical PUF.



**Figure 5.** a) FHD distributions obtained by perturbing the scatterer positions for  $\sigma$  equal to 2.0%, 8.0%, and 14.0%. The inset shows a schematic view of misplaced scatterers. b) FHD trend for the  $R'_{R_{SR\%}}$  comparison (red ribbon). The experimental “unlike” (black ribbon line) and “like” distributions (light green ribbon) are also shown for reference. c) Representative sketch about randomly removed and removed and added scatterers in new positions. d) The comparison  $R'_{R_{sc\%}}$  for different percentages of RR and RA scatterers modifications (red solid and blue dashed lines respectively). e) FHD trend for numerical “unlikes” (black (RR) and green (RA) ribbons), compared FHD distributions  $R'_{R_{sc\%}}$  (red (RR) and blue ribbons (RA)), and “like” distributions (light green ribbon) represent the reference.

This analysis has been carried out experimentally and verified by numerical calculation. The addressed case is of practical relevance assuming that the physical token must be manually inserted by a user in a slot for its optical readout. Numerically, we model the displacement by performing a translation of the geometry along the  $x$ -axis, which is modeled with periodic boundary conditions for convenience (Figure 6a). Based on the so-called memory effect for speckle patterns,<sup>[53,54]</sup> a rigid shift



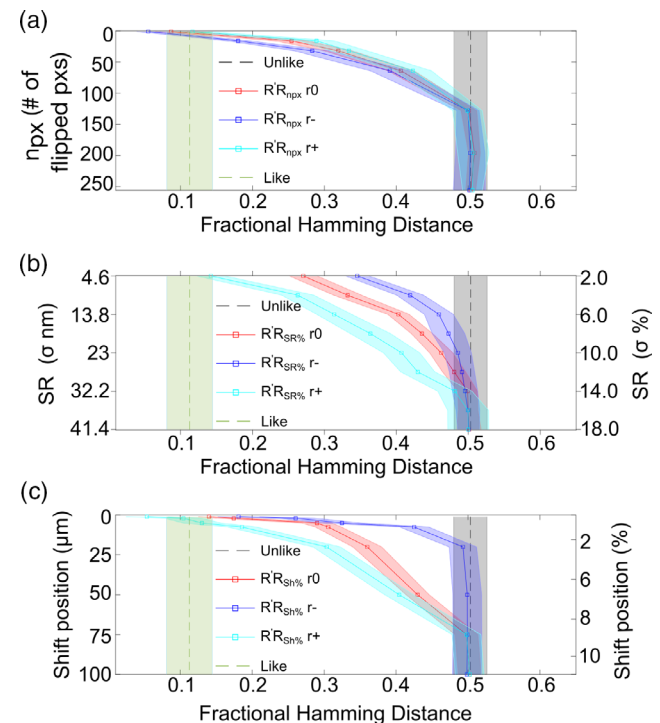
**Figure 6.** a) Illustration of the optical PUF shift with respect to initial position and the probing/readout system. b) Numerical (red dashed lines) and experimental (blue solid lines) comparisons ( $R' R_{sh\%}$ ) reported for a rigid shift along the x direction, equal to 0.1%, 2.5%, and 13%. c) Trend for numerical and experimental “unlike” distributions (black ribbon and green dots respectively), the  $R' R_{sh\%}$  comparison (red ribbon and blue hollow dots), and the experimental “like” (light green ribbon), for reference.

of the PUF should correspond to a proportional shift of the response pattern if the displacement is small. In the following sections, the applied shift (sh%) ranging from 0.13% to 13.3% has been evaluated as the ratio between the translation from 1 to 100  $\mu\text{m}$  and the lateral size of the sample (750  $\mu\text{m}$ ). We therefore expect that for small shifts, the  $R' R_{sh\%}$  FHD distributions should remain almost unaffected as long as we realign the optical responses using a registration algorithm (see Experimental Section). Numerical and experimental measurements are in good agreement and show that the compared distributions become independent (i.e., the responses are different and/or registration fails) after a shift of 0.1%, corresponding to  $\approx 1 \mu\text{m}$ , as reported in Figure 6b,c. The effect of the physical unclonable function misalignment on the speckle pattern is shown in Figure S7, Supporting Information. For the analysis presented in Figure 6, we used an interrogation with random challenges made by  $16 \times 16$  macropixels. More in general, the sensitivity to misalignment within the measurement setup depends on the size of the pixels of the challenges because the difference between the bright and dark area on the PUF, before and after the misalignment, increases when the size of the macropixels decreases. Other types of misalignment, such as rotations, could

be also handled by the same image registration algorithm up to a certain degree and could be studied in principle using the same experimental procedure and numerical tools that we proposed in this section.

### 3.4. Sensitivity to Varying Scatterers Sizes

As a final test, we numerically study how the sensitivity changes when the scatterer radius is either increased or decreased. Compared to the original hole radius of  $r_0 = 200 \text{ nm}$ , we test a reduced (subwavelength) value of  $r_- = 150 \text{ nm}$ , and  $r_+ = 400 \text{ nm}$  (hole diameter  $> \lambda$ ). The effect of this change is evaluated over the previous scenarios, including the challenge sensitivity, positional perturbation, and rigid displacement tests. The results are summarized in Figure 7, showing that increasing the hole size leads to a slightly larger PUF sensitivity to small changes in the challenge (Figure 7a), but also to a larger tolerance to fabrication imperfections (Figure 7b), highlighting a trade-off between the strength and the unclonability for the considered 2D geometry. Similarly, the last panel shows how the hole radius affects also the overall misalignment tolerance of the PUF, which can be made significantly stricter by pushing the aperture size mode deeply into the subwavelength regime. The POC values estimated for the scatterer relocation cases ( $r_+$  and  $r_-$ ) are reported in Figure S8, Supporting Information.



**Figure 7.** The robustness/tolerance tunability based on the scatterers radius: a) increasing the scatterers radius, the optical PUF becomes more sensitive to a single flip in the  $C_i$  challenge; b,c) while decreasing, it enhances the PUF sensitivity to scatterer misplacement or overall PUF misalignment (trends shown in the cyan, red, and blue ribbon lines, respectively). The black and the light green ribbons report the “unlike” and the experimental authentication threshold “like”, for reference.



## 4. Conclusion

This article quantified the sensitivity and unclonability of scattering-based optical physical unclonable functions in simulations and, for a few scenarios, also in experiments. We focused our study on 2D structures as they are very attractive for integrated devices in the visible and telecommunication range also for cryptographic applications. We analyzed several relevant scenarios, including cloning attempts, challenge sensitivity, and the tolerance to device misalignment during optical readout. Fabrication imperfections of few nm, or even the mismatch of one challenge pixel between the interrogation and the enrolled ones, are sufficient to deny the authentication. Evaluating the sensitivity of a PUF to small changes in the challenge pattern is also relevant to estimate the maximum CRP space that can be reasonably accessed using a PUF. Finally, the misalignment test, relevant in a scenario where the PUF must be aligned into an optical readout device, shows that the tolerable misalignment is smaller than 10  $\mu\text{m}$ , for a realistic detector distance of 5 mm. These parameters, properly scaled for the PUF and readout system specs, should be taken into account when designing a readout device.

At the same time, our results provide guidance on how to tune these values as needed toward either more robust or tolerant authentication devices, for example, by acting on the radius of the holes in the structure. Notably, our proposed numerical approach to test diffraction-based 2D optical PUFs is computationally efficient and flexible, allowing to investigate also other physical effects such as thermal expansion, mechanical stress, tampering attempts, and readout noise or aberrations in future works.

As a final remark, our results outline a general strategy to evaluate the sensitivity of optical physical unclonable functions under different scenarios and provide a more quantitative ground to the general assumptions regarding their resilience against adversarial attacks. Regardless of the specific 2D geometry considered here, these results are relevant also for more complex architectures with 3D disorder, since the security level of 2D devices can be reasonably taken as a lower bound to the expected security of 3D PUFs. Given the fast progress of advanced rigorous numerical methods, we envision that performing a similar analysis on a representative 3D arrangement of scatterers will soon be possible to test directly this assumption and quantify the security gain provided by multiple scattering also in other disordered 3D structures.

## 5. Experimental Section

**Sample Fabrication:** The 2D optical PUFs were experimentally fabricated by exploiting the irreproducible self-assembly of dielectric nanospheres (polystyrene) on glass substrates. The nanospheres were deposited via spin coating, in the regime of high spinning speeds (6000 rpm) where they form a monolayer with random arrangement (see Figure S3a, Supporting Information). The initial diameter of the spheres (617 nm) was then reduced by Ar plasma to about 400 nm to create a reflective mask (Figure S3b, Supporting Information) by evaporation of 80 nm of titanium (Figure S3c, Supporting Information). The spheres were then removed by sonication in isopropanol. This four-step process resulted in a 2D reflective perforated membrane with a random arrangement of nanoholes; see Figure S3d, Supporting Information.

**Optical Setup:** A He–Ne laser beam ( $\lambda = 633 \text{ nm}$ , 5 mW) propagated through lenses (L), polarizers (P), and iris (I). The beam spot (magnified by a beam expander composed of a first lens  $L_1$  the iris I and the

magnification lens  $L_2$ ) impinged on a digital micromirror device (DMD) used to generate the challenge ( $C_i$ ) to interrogate the scattering PUF sample. The challenge  $C_i$  was focused using an infinity-corrected lens ( $L_\infty$  with focal length  $f = 200 \text{ mm}$ ) into the objective backfocal plane (OB) with  $10\times$  magnification), which allowed to demagnify the challenges to a total area of  $750 \times 750 \mu\text{m}^2$  corresponding to the physical extent of the experimental PUF. The optical pattern transmitted through the perforated membrane interfered in the far field to form a speckled pattern response ( $R_i$ ), which was collected by a lens in  $2f$  configuration ( $L_{2f}$ ) far away from the PUF. Finally, the speckled pattern was recorded by a  $250 \times 250$  pixels camera (placed slightly off-axis to discard the ballistic signal) at 20 frames per second. A beam stabilizer was also included in the beam path, adjusting the beam position by means of a position detector (PD) controlling a piezoelectric mirror (PM), see Figure S1, Supporting Information.

**Numerical Simulations:** The RS method exploits a fast-Fourier transformation operation evaluating the far-field starting from the near field at a fixed distance along the light propagation direction  $z$ . Each random  $C_i$  mask was created as a chessboard with size of  $16 \times 16$  pixels filled with an equal number of “on” and “off” pixels placed randomly. The numerical sample contained a large number of scatterers ( $\approx 2 \times 10^6$  for  $f_p \approx 0.71$ ), and the generated responses were collected on a  $250 \times 250$  pixel grid as in the experiments, at a distance of  $z = 5 \text{ mm}$  and at an off-axis angle to avoid ballistic light.

**Image Registration:** To properly evaluate the tolerance of the illumination and readout process to small shifts of the PUF, we applied an image registration algorithm to both experimental and numerical responses before calculating the FHD. Due to the high sensitivity of the Gabor hashing function to small changes in the responses, we found that registering speckle patterns had a relatively small impact when trying to recover a small misalignment, showing instead a much larger reduction of the FHD when applied to larger displacement values. Beyond a certain misalignment, however, the registration step itself will eventually fail, in which case we left the alignment of  $R_i$  unmodified.

## Supporting Information

Supporting Information is available from the Wiley Online Library or from the author.

## Acknowledgements

G.E.L. and S.N. contributed equally to this work. The authors thank H. Cao for fruitful discussion and G. Roati and G. Del Pace for their help with the experimental equipment. This work was supported in part by the US Air Force Office of Scientific Research (AFOSR) under grant no. FA9550-21-1-0039 with the project “Highly Secure Nonlinear Optical PUFs”. G.E.L. and F.R. thank the Fiber-Based Planar Antennas for Biosensing and Diagnostics (FASPEC) and the project “Complex Photonic Systems (DFM.AD005.317). G.E.L. also thanks the research project “FSE-REACT EU” financed by National Social Fund, National Operative Research Program and Innovation 2014-2020 (D.M. 1062/2021). Part of this work was carried out at Nanofacility Piemonte INRiM, a laboratory supported by the “Compagnia di San Paolo” Foundation, and at the QR Laboratories, INRiM.

## Conflict of Interest

The authors declare no conflict of interest.

## Data Availability Statement

The data that support the findings of this study are openly available in Quantifying the Sensitivity and Unclonability of Optical Physical Unclonable Functions (DATA and Python codes) at 10.5281/zenodo.7142992, reference number [55]. The puffratio python code used



to generate and process the numerical data is available at the following link  
<https://github.com/lpattelli/puffraccio.git> on Github.

## Keywords

authentications, optical physical unclonable functions, Rayleigh–Sommerfeld diffraction, scattering, speckle sensitivity

Received: August 1, 2022

Revised: October 13, 2022

Published online:

- [1] U. Cisco, Annual Report of Cisco, Cisco, San Jose, CA **2020**, [https://www.cisco.com/c/dam/en\\_us/about/annual-report/cisco-annual-report-2020.pdf](https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-2020.pdf).
- [2] R. Anderson, in *Security Engineering: A Guide To Building Dependable Distributed Systems*, John Wiley & Sons, Hoboken, NJ **2020**.
- [3] P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, Y. Yarom, in *IEEE Symp. on Security and Privacy (SP)*, IEEE, Piscataway, NJ **2019**, pp. 1–19.
- [4] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, M. Hamburg, in *27th USENIX Security Symposium (USENIX Security 18)*, IEEE, Piscataway, NJ **2018**, pp. 973–990.
- [5] R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, *Science* **2002**, 297, 2026.
- [6] B. Gassend, D. Clarke, M. van Dijk, S. Devadas, in *Proc. of the 9th ACM Conf. on Computer and Communications Security*, Association for Computing Machinery, New York **2002**, p. 148–160.
- [7] U. Rührmair, D. E. Holcomb, in *Design, Automation & Test in Europe Conf. & Exhibition*, IEEE, Piscataway, NJ **2014**, pp. 1–6.
- [8] C. Herder, M.-D. Yu, F. Koushanfar, S. Devadas, *Proc. IEEE* **2014**, 102, 1126.
- [9] U. Rührmair, X. Xu, J. Sölter, A. Mahmoud, F. Koushanfar, W. Burleson, *Cryptol. ePrint Arch.* **2013**.
- [10] U. Rührmair, *J. Cryptograph. Eng.* **2022**, 1.
- [11] J. Das, K. Scott, S. Rajaram, D. Burgett, S. Bhanja, *IEEE Trans. Nanotechnol.* **2015**, 14, 436.
- [12] G. E. Suh, S. Devadas, in *2007 44th ACM/IEEE Design Automation Conf.*, IEEE, Piscataway, NJ **2007**, pp. 9–14.
- [13] P. H. Nguyen, D. P. Sahoo, C. Jin, K. Mahmood, U. Rührmair, M. van Dijk, *Cryptol. ePrint Arch.* **2018**.
- [14] P. Lugli, A. Mahmoud, G. Csaba, M. Algasinger, M. Stutzmann, U. Rührmair, *Int. J. Circuit Theory Appl.* **2013**, 41, 619.
- [15] G. Csaba, X. Ju, Z. Ma, Q. Chen, W. Porod, J. Schmidhuber, U. Schlichtmann, P. Lugli, U. Rührmair, in *12th Int. Workshop on Cellular Nanoscale Networks and their Applications*, IEEE, Piscataway, NJ **2010**, pp. 1–6.
- [16] G. DeJean, D. Kirovski, in *International Workshop On Cryptographic Hardware And Embedded Systems*, Springer, New York **2007**, pp. 346–363.
- [17] S. A. Goorden, M. Horstmann, A. P. Mosk, B. Škorić, P. W. H. Pinkse, *Optica* **2014**, 1, 421.
- [18] R. Uppu, Tom A. W. Wolterink, S. A. Goorden, B. Chen, B. Škorić, A. P. Mosk, P. W. H. Pinkse, *Quant. Sci. Technol.* **2019**, 4, 045011.
- [19] B. Škorić, P. Tuyls, W. Oprey, in *Int. Conf. On Applied Cryptography and Network Security*, Springer, New York **2005**, pp. 407–422.
- [20] P. Tuyls, B. Škorić, T. Kevenaar, in *Security With Noisy Data: On Private Biometrics, Secure Key Storage And Anti-Counterfeiting*, Springer Science & Business Media, New York **2007**.
- [21] R. Horstmeyer, B. Judkewitz, I. M. Vellekoop, S. Assaworrorarit, C. Yang, *Sci. Rep.* **2013**, 3, 3543.
- [22] P. Wang, F. Chen, D. Li, S. Sun, F. Huang, T. Zhang, Q. Li, K. Chen, Y. Wan, X. Leng, Y. Yao, *Phys. Rev. Appl.* **2021**, 16, 054025.
- [23] R. Horstmeyer, S. Assaworrorarit, U. Rührmair, C. Yang, in *IEEE Int. Symp. on Hardware Oriented Security and Trust (HOST)*, IEEE, Piscataway, NJ **2015**, pp. 157–162.
- [24] J. Feng, W. Wen, X. Wei, X. Jiang, M. Cao, X. Wang, X. Zhang, L. Jiang, Y. Wu, *Adv. Mater.* **2019**, 31, 1807880.
- [25] N. Kayaci, R. Ozdemir, M. Kalay, N. B. Kiremitler, H. Usta, M. S. Onses, *Adv. Funct. Mater.* **2022**, 32, 2108675.
- [26] T. Ritacco, G. E. Lio, X. Xu, A. Broussier, A. Issa, M. Giocondo, R. Bachelot, S. Blaize, C. Couteau, S. Jradi, *ACS Appl. Nano Mater.* **2021**, 4, 6916.
- [27] K. Kim, S. Bittner, Y. Zeng, S. Guazzotti, O. Hess, Q. J. Wang, H. Cao, *Science* **2021**, 371, 948.
- [28] G. E. Lio, A. D. Luca, C. P. Umeton, R. Caputo, *J. Appl. Phys.* **2020**, 128, 093107.
- [29] J. Berk, M. R. Foreman, *ACS Photon.* **2021**, 8, 2227.
- [30] J. Berk, C. Paterson, M. R. Foreman, *J. Lightwave Technol.* **2021**, 39, 3950.
- [31] A. Ferraro, M. D. L. Bruno, G. Papuzzo, R. Varchera, A. Forestiero, M. P. De Santo, R. Caputo, R. C. Barberi, *Nanomaterials* **2022**, 12, 1279.
- [32] B. R. Anderson, R. Gunawidjaja, H. Eilers, *Appl. Optics* **2017**, 56, 2863.
- [33] V. Caligiuri, A. Patra, M. P. De Santo, A. Forestiero, G. Papuzzo, D. M. Aceti, G. E. Lio, R. Barberi, A. De Luca, *ACS Appl. Mater. Interfaces* **2021**, 13, 49172.
- [34] F. B. Tarik, A. Famili, Y. Lao, J. D. Ryckman, *Nanophotonics* **2020**, 9, 2817.
- [35] B. C. Grubel, B. T. Bosworth, M. R. Kossey, H. Sun, A. B. Cooper, M. A. Foster, A. C. Foster, *Opt. Express* **2017**, 25, 12710.
- [36] J. Knechtel, J. Goscinia, A. Bojesomo, S. Patnaik, O. Sinanoglu, M. Rasras, *Journal of Lightwave Technol.* **2019**, 37, 3805.
- [37] Q. Li, F. Chen, J. Kang, P. Wang, J. Su, F. Huang, M. Li, J. Zhang, *Adv. Photon. Res.* **2022**, 3, 2100207.
- [38] J. D. R. Buchanan, R. P. Cowburn, A.-V. Jausovec, D. Petit, P. Seem, G. Xiong, D. Atkinson, K. Fenton, D. A. Allwood, M. T. Bryan, *Nature* **2005**, 436, 475.
- [39] Q. Li, F. Chen, M. Li, H. Long, P. Sun, P. Wang, Y. Yao, J. Zhang, *Opt. Quantum Electron.* **2017**, 49, 122.
- [40] R. Maes, I. Verbauwhe, in *Towards Hardware-Intrinsic Security*, Springer, New York **2010**, pp. 3–37.
- [41] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, R. J. Young, *Appl. Phys. Rev.* **2019**, 6, 011303.
- [42] F. J. Torcal-Milla, L. M. Sanchez-Brea, *Opt. Laser Technol.* **2017**, 97, 316.
- [43] L. M. Sanchez-Brea, F. J. Torcal-Milla, J. Buencuerpo, *Opt. Laser Technol.* **2018**, 107, 337.
- [44] L. M. Sanchez-Brea, F. J. Torcal-Milla, J. del Hoyo, A. Cuadrado, J. A. Gomez-Pedrero, *J. Optics* **2020**, 22, 065601.
- [45] G. E. Lio, A. Ferraro, T. Ritacco, D. M. Aceti, A. D. Luca, M. Giocondo, R. Caputo, *Adv. Mater.* **2021**, 33, 2008644.
- [46] M. Skoge, A. Donev, F. H. Stillinger, S. Torquato, *Phys. Rev. E* **2006**, 74, 041127.
- [47] F. Riboli, F. Uccieddu, G. Monaco, N. Caselli, F. Intonti, M. Gurioli, S. E. Skipetrov, *Phys. Rev. Lett.* **2017**, 119, 043902.
- [48] J. Daugman, *Pattern Recogn.* **2003**, 36, 279.
- [49] M. S. Kim, G. J. Lee, J. W. Leem, S. Choi, Y. L. Kim, Y. M. Song, *Nat. Commun.* **2022**, 13, 247.
- [50] C. Mesaritakis, M. Akriotou, A. Kapsalis, E. Grivas, C. Chaintoutis, T. Nikas, D. Syvridis, *Sci. Rep.* **2018**, 8, 9653.
- [51] A. Anastasiou, E. I. Zacharaki, A. Tsakas, K. Moustakas, D. Alexandropoulos, *Sci. Rep.* **2022**, 12, 2891.

- [52] F. B. Tarik, A. Famili, Y. Lao, J. D. Ryckman, *Sci. Rep.* **2022**, *12*, 15653.
- [53] S. Feng, C. Kane, P. A. Lee, A. D. Stone, *Phys. Rev. Lett.* **1988**, *61*, 834.
- [54] H. Yilmaz, M. Kühmayer, C. W. Hsu, S. Rotter, H. Cao, *Phys. Rev. X* **2021**, *11*, 031010.
- [55] G. E. Lio, S. Nocentini, L. Pattelli, E. Cara, D. S. Wiersma, U. Rührmair, F. Riboli, Quantifying the Sensitivity and Unclonability of Optical Physical Unclonable Functions (DATA and Python codes), <https://zenodo.org/record/5986425>.