All-optical multilevel physical unclonable functions

Publisher version: https://www.nature.com/articles/s41563-023-01734-7#article-info

Final accepted version

DOI: 10.1038/s41563-023-01734-7

All-optical multi-level Physical Unclonable Functions

Sara Nocentini*[1,2], Ulrich Rührmair[3,4], Mauro Barni[5], Diederik S. Wiersma[1,2,6], Francesco Riboli*[2,7]

[1] Istituto Nazionale di Ricerca Metrologica, Strada delle Cacce 91, 10135 Torino, Italy; [2] European Laboratory for Nonlinear Spectroscopy, Via Nello Carrara 1, 50019 Sesto Fiorentino (FI), Italy; [3] Electrical Engineering and Computer Science Department, TU Berlin, 10623 Berlin, Germany; [4]Electrical and Computer Engineering (ECE) Dept., University of Connecticut, Storrs, CT, USA; [5] Dipartimento di Ingegneria dell'Informazione e Scienze Matematiche, Università di Siena, via Roma 56, 53100 Siena; [6] Dipartimento di Fisica, Università di Firenze, Via Sansone 1, 50019, Sesto Fiorentino, Italia; [7]CNR-INO, Via N. Carrara 1 Sesto Fiorentino, 50019, Italy;

*nocentini@lens.unifi.it; riboli@lens.unifi.it

Disordered photonic structures are promising for the realization of physical unclonable functions (PUF) – physical objects that can overcome the limitations of conventional digital security and can enable cryptographic protocols immune against attacks by future quantum computers. The physical configuration of traditional PUFs is either fixed or can only be permanently modified, allowing one token per device and limiting their practicality. Here, we overcome this limitation by creating reconfigurable structures made by light-transformable polymers in which the physical structure of the unclonable function can be reconfigured reversibly. Our approach allows the simultaneous co-existence of multiple physical unclonable functions within one device. The physical transformation is done all-optically in a reversible and spatially controlled fashion, allowing the generation of more complex keys. At the same time, as a set of switchable individual PUFs, it enables the authentication of multiple clients and allows for practical implementations of quantum-secure authentication and nonlinear generators of cryptographic keys.

Complex photonic systems[1–4] are characterized by a multitude of spatial degrees of freedom that, in the presence of coherent light, produce a complex intensity pattern (called speckle) as the result of interference of a large number of independent transmission channels[5]. Speckle is extremely sensitive to minute changes in the physical structure of the material[6,7] – to the level that it is nearly impossible to clone disordered structures and obtain the same optical response without resorting to techniques at the molecular level[8]. These characteristics make them ideal candidates for cryptographic primitives such as physical unclonable

functions for authentication and communication purposes [9-11]. Electrical – in contrast to optical – strong PUFs have been examined intensively[10,12] and most of them have been attacked successfully via various digital and physical techniques over the years[13]. Optical PUFs, with their elevated three-dimensional complexity and entropy levels, receive currently much attention for potential applications[10] in cryptographic key generation[14] and anticounterfeiting of goods[15].

The growing scientific and industrial interest in the security of goods and the protection of sensitive data and services fosters two main research lines. Different chemical-physical processes [16-20] have been harnessed for anti-counterfeiting labels while 3D complex photonic media and integrated photonic circuits [21-23] have been tested as cryptographic key generators (strong PUFs) for enhancing the security of authentication processes.

Optical strong PUFs have been introduced by Pappu[24] with the name of Physical One-Way Functions. This first instantiation was limited in stability and reproducibility, while in later works the use of spatial[25,26] or spectral[27] modulators provided a significant improvement. This implementation relies on static hardware whose properties cannot be reconfigured in case of a detected attack. Kursawe et al. showed that permanent modifications can be created by melting the polymer aggregates, creating a net entropy decrease in every new reconfiguration [28]. Horstmeyer and coauthors showed that it is possible to reconfigure an optical PUF by exploiting electrical driven polymer dispersed liquid crystals[26] and John et al. managed to do this electrically by using halide perovskite memristors[29]. A recent alternative for reconfigurable PUF exploits the stochastic crystallization of a supersaturated sodium acetate solution that provides reusable and time-efficient cryptographic key generators[30]. In all these cases, the internal states cannot be recovered after reconfiguration[26]. To increase the information entropy, it is necessary to provide a reversible transformation among the possible microscopic configurations. A preliminary result in this direction was obtained by Gan and coauthors, who reported that the temperature-controlled phase transition of Vanadium oxide nanocrystals can be used to create reversible switching among two states (crystalline and amorphous) [31].

In order to increase the complexity (entropy) and introduce a reversibly reconfigurable system, it is necessary to provide complex photonic materials with a reversible transformation of the scattering potential. Among the reconfigurable materials, dye doped polymer dispersed and stabilized liquid crystals offer a spatial temporal control of the scattering potential which can be made hysteresis-free by customization of their chemical composition. In this way, we obtained optical physical unclonable functions characterized by a net increase of entropy and which integrate multiple cryptographic functions in a single device.

The concept of multi-level PUF

We introduce a concept and technology platform that provides interchangeable multi-level operation by reversibly transforming the scattering properties of a complex photonic medium based on photosensitive polymeric film. The operation principle of this cryptographic primitive – that we term Hyper PUF (HPUF) – is illustrated in Fig. 1. A "standard" PUF (left panel of Fig. 1) is characterized by an authentication process via a single challenge C_i^{Probe}, while the HPUF (right panel of Fig. 1) is interrogated by a challenge $C_{ik} = (C_i^{Probe}, L_k^{Trans})$ consisting of two sub-challenges. First, a configuration pattern L_k^{Trans} (a spatially modulated parametric matrix) transforms the internal configuration between different levels in an all-optical and reversible manner and determines the scattering potential of the associated HPUF level. Secondly, a standard interrogation challenge C_i^{Probe} produces a measurable unique optical interference pattern as PUF response $R_{ik}(C_i^{Probe}, L_k^{Trans})$. Mathematically, the HPUF can be modeled as a parametric function that maps its domain to a larger codomain, whose dimension depends not only on the number of C_i^{Probe} but also on the number of transformer challenges L_k^{Trans}, $f: (C_i^{Probe}, L_k^{Trans}) \rightarrow R_{ik}$. The same internal configuration can be restored by applying the same transformer challenge, allowing back-and-forth switching between the

PUF's internal levels. This marks a significant difference between HPUFs and existing reconfigurable PUF designs,[26,29] in which internal changes are permanent and non-reversible.

The practical usage of physical unclonable functions in authentication processes is governed by a registration and verification protocol of the challenge-response-pairs[32] that for standard and HPUFs differs in the library dimensionality and the type of challenge sent to the claimant (see Supplementary Note 1 and Supplementary Fig. 1). In our analysis, to discriminate between legitimate and fraudulent authentication requests, we estimate the similarity of two binary keys by the fractional hamming distance (FHD) – that is the percentage of bits that differs between two binary strings [33]. The distribution between the responses to the same challenge (*like* FHD) quantifies the stability of the system, while that one between the responses to different random challenges (*unlike* FHD) is used to evaluate possible correlation among the responses. We refer to intra-device FHDs when comparing responses from the same PUF or inter-device FHDs when comparing responses from different PUFs. Following the method introduced by Daugman [33], the number N of independent bits (the entropy) of the generated keys can be estimated by $N = \frac{p*(1-p)}{\sigma^2}$, where p is the mean value and σ the standard deviation of the distribution (Methods [33,34]). This is a crucial parameter in the security metrics since it directly relates to the resilience against different types of attacks: a large entropy ensures a higher level of security against brute force, modeling and side channel attacks.

All-optical transformation of the microscopic structure

The HPUF is a 3D disordered photonic medium that is responsive to the transformer challenge while unperturbed to the probing challenge. It consists of a polymeric film (polydimethylsiloxane) where stabilized liquid crystal (LC) droplets are randomly dispersed via an emulsion process (Methods) resulting in polymer dispersed and polymer stabilized liquid crystals[35] as shown in Fig. 2a. The resulting polymeric film is flexible, elastic and can conformally adhere to different types of substrates (Supplementary Fig. 2). For authentication protocols, we placed the polymeric film on a flat transparent substrate that can be inserted in a 3D printed authentication card as shown in Fig. 2a. The selective response to the transformer challenges is achieved by doping the common liquid crystal 5CB (pentyl-cyano-biphenyl) with a blue absorbing dye (dispersed red 1, DR1). Blue incoherent light (L_k^{Trans}) transforms the internal state by absorbing light via the chromophore and thereby generating a temperature driven LC phase transition, while red coherent light (C_i^{Probe}) probes the transformed PUFs. The nematic isotropic transition temperature of the dye-doped stabilized LC is around $T_{N\text{-}I}$=32°C (Supplementary Fig. 3). By choosing a different liquid crystal mesogen or by modifying the chemical formulation, the $T_{N\text{-}I}$ can be customized in order to meet specific needs. The minimum size of macropixel (detail) of the transforming challenge, finally determining the total number of HPUF levels, should be chosen larger than the polymer thermal diffusion length (Methods). Fig. 2g-h shows the thermal maps of the HPUF illuminated with a 4x4 macro-pixel checkerboard transforming challenge. The local temperature increases in time, eventually reaching a steady state thermal conduction after around 20 sec. At the equilibrium, the temperature of the illuminated area is above the nematic-isotropic transition temperature $T_{N\text{-}I}$ (horizontal red dotted line), locally inducing the LC phase transition. The selective spatial modulation of the scattering potential is lost by decreasing the size of the macro-pixel of the transformer challenge (Supplementary Fig. 4). To increase the number of levels that are currently limited by thermal diffusion, we can use a switching mechanism based on azobenzene dye isomerization with similar temporal dynamics[36] or refractive index changes based on third-order non-resonant nonlinearity that induces reorientation of the molecules on a millisecond time scale under high-power laser illumination[37].

To guarantee the full reversibility of the realignment process, the LC droplets are stabilized with cross linker molecules (Fig. 2a) that create a fixed polymeric network[38] as shown in Fig. 2d-f. The presence of the cross linker molecules guarantees an hysteresis-free process with a fully reversible switching between

two LC phases[39]. The transformation between different internal configurations is deterministic, stable, and repeatable, regardless of the history of the system.

Increase of entropy

The experimental characterization is illustrated in Fig. 3a. The system is illuminated with the challenge C_i^{Probe} that is generated by modulating the Gaussian wavefront of an He-Ne laser using a digital micro-mirror device (DMD) [41,42]. Light is then scattered by the HPUF, generating in the far field the response R_{ik} (the speckle pattern) – a 2D image whose spatial features depend uniquely on the probe C_i^{Probe} and transform challenge L_k^{Trans} of the system. The response R_{ik} is imaged on a CCD camera, then filtered and binarized to generate the key. The raw speckle images (the optical responses R_{ik}) are converted into binary keys by using a Gabor filter to remove pixel-scale noise, averaging the undesired intensity variations and extracting the independent bits[24]. The parameters of the Gabor filter have been tuned in order to maximize the extractable entropy from the PUF response (Supplementary Fig. 5). The filtering of the raw response images affects the information content intrinsically encoded in the speckle patterns, but is necessary for creating highly entropic and noise-robust binary keys that can be used along an authentication process between parties. Switching between the levels of the HPUF is triggered by the bright blue profile L_k^{Trans} (spatially overlapping the bright red challenge C_i^{Probe}).

The characterization has been performed by evaluating the entropic content of the keys as the number of independent bits generated by an increasing number of levels: from one-single level PUF up to a ten-level HPUF. The encoding capacity of the systems then depends on the independent bits N of the single level (2^N) and it is expected to have a polynomial growth when considering multiple levels (Methods) up to a maximum of 10^N, in case of no correlations among the responses of the levels. This statistical analysis typically performed using the Daugman's method[24] can also be verified using alternative strategies such as the equivalent Markov chain entropy estimation[33] or the statistical tests provided by the National Institute of Standards and Technology (NIST), such as the NIST suite 800-90B[43].

We firstly characterize the one-single level system by interrogating the HPUF with challenges (C_i^{Probe}, L^{Trans}=0) with i={1,…,100}. Fig. 3b shows that the *like* and *unlike* FHDs distributions are well separated, and that the authentication threshold can be safely set around 0.35. The number of independent bits of the generated keys is estimated to be N_{1Level}=*928* bits (Methods). The characterization of the inter-device FHD of the one-level HPUF is reported in Supplementary Fig. 6.

The next step is to characterize the two-level HPUF for which the first level is obtained by completely shading the blue light, while the second level is configured by illuminating the PUF with a uniform blue wavefront. The responses of the two levels interrogated with the same challenge are well decorrelated and also reproducible (Fig. 3c and Supplementary Fig. 7 for the correlation map between multiple levels). The *like* and *unlike* distributions do not overlap (Fig. 3d) and the authentication threshold can be set around 0.4. We also observe a net gain in the independent bits (entropy) of the keys generated by the two-level HPUF with respect to the one-level case, from N_{1Level}= 928 bits to $N_{2Levels}$= 1323 bits (Figs. 3b and 3d).

The natural question that arises is whether, and to which extent, a further increase in the number of levels increases the entropy. To investigate this problem (which is affected by thermal diffusion, see Fig. 2g-h), we first investigated the transforming challenge details that induce a relevant decorrelation of the responses in presence of the same probing challenge. By using a checkerboard transforming challenge and its complementary image, the correlation of the responses has been evaluated (Fig. 4). The Pearson correlation coefficients of the responses (keeping the probing challenge fixed) increase by decreasing the dimension of the macro-pixel. In order to have minimally correlated responses for different transforming challenges and a good number of levels, we chose a 4x4 macro-pixel transforming challenge.

We then defined a set of 10 transformer challenges (L_k^{Trans}, with k={1,..,10}) by choosing 10 elements of the Walsh-Hadamard binary basis as a subset of a complete 16 orthogonal set of 4x4 macropixel images. Each level is interrogated with the same set of randomly selected challenges C_i^{Probe} with i={1,.., 100}(Fig. 5a) The raw responses of the HPUF and their relative post-processed bit sequences are reported in Supplementary Fig. 8. The whole codomain of responses R_{ik} can be compartmentalized by randomly joining the codomains of individual levels. For each compartment, we evaluate the entropy per symbol, that is the entropy per bit. Fig. 5b shows that the number of independent bits is around 950 (0.14 bit/bit). This value is almost independent of the chosen level (in this case, each compartment is composed by the codomain of a single level). By populating the compartments with the codomains of more levels (up to ten), the entropy of the generated key increases up to around $N_{10Levels}$= 1750 bits that correspond to 0.24 bit/bit (Fig. 5b, left panel, red circles). Therefore, a HPUF with 10 levels has an encoding capacity of 2^{1750}, which is much larger than that obtained for the single-level (standard) PUF that is 2^{928}.

The increase of the entropy per symbol evaluated by the Daugman's analysis is confirmed by modeling the extracted keys with equivalent Markov chains, generated via transition matrices whose coefficients represent the permanence and transition probabilities of the binary values of the keys. The entropy per symbol of the Markov chains is then calculated analytically[33] (Methods and Supplementary Fig. 9). The analysis of the experimental data with two models shows the same entropic trend suggesting that the different levels behave like different cryptographic primitives coexisting in the same hardware.

To validate this idea, we fabricated ten different cryptographic primitives. We applied the same compartmentalization scheme making an analogy among each codomain of ten different PUFs and each codomain of the ten levels of the HPUF. We observe that the entropy of the generated keys as a function of the number of PUFs, has absolute values and a dependence qualitatively similar to the HPUF (Fig. 5b, left panel, black circles). This is the confirmation that the transformer challenges L_k^{Trans} induce different microscopic configurations in the same region of the sample, mimicking different PUFs.

It is important to notice that the entropy increase does not depend on the number of responses but only on the number of levels of the HPUF. Increasing the number of responses but considering a single configuration, the entropy per symbol remains constant (Supplementary Fig. 10).

By analyzing the properties of the equivalent Markov chains, we observe that the increase of the number of levels leads to permanence and transition (α and 1-α respectively) probabilities of the Markov transition matrix, that tend towards a situation of equiprobability (α = 0.5) as shown in Supplementary Fig. 11. This implies the reduction of the correlation length in the bit sequence (Fig. 5c-d), and consequently an increase in the entropy of the key (Supplementary Fig. 9b and 12). Indeed, the correlation length of the bit sequence gets shorter and shorter when increasing the number of levels (Fig. 5c), until it reaches an asymptotic value and the entropy per symbol saturates. The physical origin of the increase in the entropy per symbol is due to an increase of the microscopic configurations of the system probed by the challenge C_i^{Probe}, that translates in an increase of the variety of speckle patterns that form the codomain of the HPUF. The growing rate of the entropy is reduced up to a saturation level when the compartment is populated by roughly 8-10 levels. This saturation can be associated with the limited number of light transmission channels for a given set of interrogation challenges and for a given set of detail of the transforming challenge. The entropy per symbol saturates when light key-vectors probes all the possible accessible configurations of the system (Supplementary Note 2).

Outlook

We developed optical cryptographic primitives, which we term Hyper Physical Unclonable Functions, that allow all-optical multi-level operation thanks to fully reversible switching of the optical properties of a

flexible polymer dispersed and stabilized liquid crystal film. The entropy - and therefore the security against cyber-attacks[45,46] - increases with the number of levels (or internal configurations) that coexist within one and the same sample boosting integration and cloning resilience. The device stores in the material properties the operation of multiple physical unclonable functions that can be switched only with an appropriate light stimulus making cloning of the different internal molecular states impossible.

The choice of materials and the multi-level authentication enable a wide range of practical applications which take advantage of the reversibly reconfigurable and customizable optical properties. The spatial-temporal transformation of the scattering potential represents a promising solution not only as a primitive for multi-user or multi-process authentication but also for quantum secure authentication[47,48] and nonlinear optical functions for cryptography and photonics[49].

Our films constitute an easily tailorable hardware whose fabrication parameters determine optical properties such opacity, that we evaluate as $ln\ (I_{in}\ /\ I_{out})$ (Fig. 6). Opacity can be varied from semi-transparent to strongly opaque by tuning the LC concentration, sample thickness and by doping with high refractive index particles. Reversibly switching among different microscopic configurations of semi-transparent films can be explored for quantum readout methods[47,48], such as the proposed quantum secure authentication of classical data (QSA-d) or quantum secure authentication of quantum data via physical unclonable functions (Fig. 6b, bottom scheme). A Hyper Physical Unclonable Function can offer a large number of levels for the authentication of data up to a decimal classical alphabet or up to a qudit with at least d=10 units of quantum information.

Opaque systems with a switchable scattering potential will allow for the experimental implementation of a random potential with a strong nonlinear optical response[49]. Nonlinear cryptographic key generators would provide much higher resilience against machine learning attacks[50], and more in general can be used as a nonlinear optical complex function in optical computing and machine learning.

Acknowledgements

The research leading to these results has received funding from AFOSR/RTA2 (A.2.e. Information Assurance and Cybersecurity) project “Highly Secure Nonlinear Optical PUFs” (FA9550-21-1-0039) awarded to U.R, Ente Cassa di Risparmio di Firenze (2018/1047) awarded to F.R., and Fondo premiale FOE project “Volume photography: measuring three dimensional light distributions without opening the box” (E17G17000300001). This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union – NextGenerationEU and cofunded by the European Union - NextGeneration EU, "Integrated infrastructure initiative in Photonic and Quantum Sciences" - I-PHOQS [IR0000016, ID D2B8D520, CUP B53C22001750006] awarded to F.R.. The authors thank Prof. Hui Cao, Dr. Yaniv Eliezer, Dr. Giuseppe Emanuele Lio, Michael Lachner, Nils Wisiol, and Adomas Baliuka for feedback on the data within the AFOSR project. We thank Dr. Daniele Martella for discussions on chemistry and Prof. Pepijn Pinkse for his inputs on the quantum secure authentication protocols.

Author Contributions Statement

S.N., F.R. and U.R. conceived the experiment. S.N. fabricated the devices. S.N. performed the characterization and the measurements. S.N. analyzed the data. M.B. and D.S.W. helped with the data

interpretation on the information theory aspects and scattering properties respectively. U. R. helped with the security and PUF-related aspects. F.R. wrote the theoretical discussion. F.R. supervised the project. S.N. and F.R. wrote the paper, and all authors discussed the results and worked on the paper.

Competing Interests Statement

The authors declare no competing interests.

Figure Legends/Captions

Figure 1. Schematic representation of the interrogation process for standard and Hyper PUFs. Working mechanism of the deterministic behavior for the challenge response pair generation for standard PUFs (left panel) and HPUFs (right panel). For the standard PUF, the challenge C_i^{Probe} probes the only possible internal configuration of the hardware, producing only one response R_i. In the HPUF, each configuration pattern L_k^{Trans} reversibly transforms the PUF level into a new one, producing different k responses R_{ik} to a given challenge C_i^{Probe}.

Figure 2. Polymer dispersed and polymer stabilized liquid crystals. a) Scheme of the polymeric film used as disordered photonic medium to realize the HPUF. As proof of concept device, the HPUF has inserted in a 3D printed authentication card (central panel). It is composed by LC droplets, whose molecular composition is reported on the left, that are randomly dispersed into the polymeric matrix (polydimethylsiloxane, PDMS). The polymer stabilized LC formulation is made by a mesogen (5CB), a chromophore (Dispersed Red 1, DR1), and a bi-acrylate (cross-linker) mesogen. A scanning electron microscope image of the side view of the film is reported on the right. b-c) Representative scheme of the molecule arrangement inside the PD&SLC droplets. b) Scheme of the LC molecular arrangement within the droplets in the nematic and c) isotropic phase. d-f) Polarized Optical Microscope images of the PD&SLC before (d), during (e) and after (f) the blue light illumination, whose area is indicated by the dashed blue circle. The four dot cross pattern (d) is a signature of the LC radial alignment in each droplet[40] and it is lost under blue laser illumination. This is the indication that the stabilized LC polymer does not prevent full LC disordering to the isotropic phase. Once the blue illumination is removed (e), the system evolves in around 10 seconds to the previously aligned configuration with the same four dot feature that was present before the transformation (as highlighted by the green circles in f). The scale bars are 10 μm in length. g) Thermal imaging of the HPUF under blue light illumination with a checkerboard shape with 4x4 macro-pixels. h) Temperature profile along the black dashed line of the panel g. Within the illuminated areas the temperature rises above the nematic to isotropic transition temperature.

Figure 3. **Hyper PUF characterization: one and two-level operation.** a) Schematics of the HPUF characterization setup where a binary challenge C_i^{Probe} is incident on the physical hardware. The transmitted intensity profile R_{ik} is collected in the far field by a CCD camera and successively converted into a binary post-processed key. A second light beam L_k^{Trans}, generated by a blue LED and spatially modulated by a DMD (integrated on a projector board), is used to reversibly transform the HPUF. Among the RGB colors of the projector, the blue LED was chosen as it better matches the dye absorption peak. The two optical images are overlapped on the token. b) Characterization of one-single level of the HPUF. The mean value of the *like* FHD shows that, on the average, the 12% of the bit between two keys generated by the same challenges are different. The test has been made with 400 challenges. The *unlike* FHD (orange histogram) is the result of 79800 pairwise comparisons that results from all possible comparisons of the 400 responses to random challenges. On average, each pair of generated keys differs in the 50% of its bits and the number of the independent bits is N_{1Level} =928 bits. c) Temporal evolution of the Pearson correlation coefficient between two raw responses (two speckle images) acquired every two seconds by interrogating the sample with the same challenge C_i^{Probe} while switching the configuration beam between L_1^{Trans} and L_2^{Trans}. The three curves correspond to three different values of the blue-light intensities (60, 85, 105 mW/cm^2), indicating that higher intensities induce a more efficient decorrelation as well as faster dynamics. We observe a full recovery of the LC alignment after every LC phase transition. d) *Like* and *unlike* FHDs of the HPUF for a two-level configuration (intensity: 85mW/cm^2). The number of the independent bits of the generated key is N_{2Level} =1323 bits. In the inset, we report the responses for the two transformer challenges L_1^{Trans} and L_2^{Trans} to two different challenges, C_1^{Probe} and C_2^{Probe}.

Figure 4. Pearson correlation coefficient (PCC) of the responses (speckle patterns). The blue points report the PCC of the response to two complementary transforming challenges (L^{Trans}), the green ones the PCC of the responses obtained with and without the transforming level and the red ones the stability of the transformation (PCC of the responses to the same transforming level in consecutive iterations). The reported data are presented as mean PCC values and their standard deviation of 5 responses comparison. All the responses refer to the same probing challenge that has been kept fixed for this analysis. On the top of the graph, optical images of the blue transformer checkerboard (the pink color is due to the overlapping with the red probing challenge). On the left and right panels, the speckle patterns to levels made by 9x9 and 2x2 macropixels, respectively. In case of a 2x2 macro-pixel (3.5x3.5 mm^2) transforming challenge, the PCC of the responses to the complementary checkerboards is as low as the correlation among the responses obtained for a two level HPUF (speckle patterns on the right of Fig. 4), while decreasing the size of the macropixel of the L^{Trans}, the PCC raises up to the stability level of the system for a 9x9 macro-pixel L^{Trans} (speckle patterns on the left of Fig. 4). In this case, the responses in presence of the complementary transforming challenges are highly correlated because the checkerboard and its complementary generate an uniform temperature profile that drives the phase transition of the whole sample.

Figure 5. Hyper PUF characterization. a) Scheme of the domain (C_i^{Probe}, L_k^{Trans}) and the codomain R_{ik} of the HPUF. The whole codomain can be compartmentalized by joining the responses of different levels. b) Entropy per symbol for different compartments of the HPUF codomain. The left panel (blue circles) shows the mean entropy per symbol for each single level (the horizontal labels show the Hadamard basis configuration patterns). The right panel shows the increase of the entropy per symbol by randomly joining the codomains of individual levels (black circles). Red circles refer to the same analysis performed by populating the compartment by joining the responses of different PUFs. The blue mean value and error bars (standard deviation) refer to 10 different characterizations of each single level. The black and red points and error bars refer to the mean value and standard deviation calculated over ten different random selections of the PUF or levels of HPUF, respectively. c) Autocorrelation of the bit sequences generated by equivalent Markov chain. The correlation length decreases as the number of levels increases, because the permanence probability of the equivalent key increases from $\alpha = 0.07$ to $\alpha = 0.12$. d) Representation of the binary keys generated by the equivalent Markov chains for one level ($\alpha = 0.07$) and ten levels ($\alpha = 0.12$).

Figure 6. Hyper PUF engineering and potential applications. Opacity is defined as the natural logarithm of the total transmittance of different HPUFs as a function of the physical thickness and concentration of TiO_2 nanoparticles. The transmittance data have been measured for 5 points and the resulting mean value and error calculated as the standard deviation are reported **(**a). A small concentration of LC droplets (less than 5% in weight of the PSLC with respect to the transparent PDMS) and HPUF thinner than 150 μm result in a semi-transparent sample, while opaque samples can be obtained for thicknesses of 170 μm (see insets). To further increase the number of scattering events in the cryptographic functions, high refractive index particles such as titanium dioxide (TiO_2 nanoparticles) have be added in a small percentage in the PDMS to increase the opacity (yellow and blue scatters). For $\ln (I_{in}/I_{out})<1$ the system looks transparent or semitransparent, being in the limit of the single scattering regime (sample labeled with 1 and 2 in the top of the panel). In this regime, the scattered light has an almost linear dependence from the scattering potential and the system can be, in principle, prepared in a classical superposition of levels, that can be interrogated with both classical or quantum state of light. This allows the implementation of recent proposed schemes of authentication and communication of data with quantum read-out PUFs[10] (panel b) bottom). For $\log (I_{in}/I_{out})>1$ the system looks opaque since the light is scattered multiple times and potentially partially absorbed. In this regime, the relationship between the scattered light and the scattering potential is not more linear[65], opening new routes in the field of nonlinear cryptography. The nonlinear dependence of the responses with respect to the scattering potential that in HPUF is controlled by the configuration levels is schematized in panel b, top part.

References

1. Vynck, K., Burresi, M., Riboli, F. & Wiersma, D. S. Photon management in two-dimensional disordered media. *Nat Mater* 11, 7–12 (2012).
2. Wiersma, D. S. Disordered photonics. *Nat Photonics* 7, 188–196 (2013).

3. Cao, H., & Eliezer, Y. Harnessing disorder for photonic device applications. *Appl Phys Rev* 9, 011309 (2022).
4. López, C. The true value of disorder. *Adv Opt Mater*, 6, 1800439 (2018).
5. Mosk, A. P., Lagendijk, A., Lerosey, G. & Fink, M. Controlling waves in space and time for imaging and focusing in complex media. *Nat Photonics* 6, 283–292 (2012).
6. Berkovits, R. Sensitivity of the multiple-scattering speckle pattern to the motion of a single scatterer. *Phys Rev B* 43, 8638 (1991).
7. Riboli, F. et al. Tailoring Correlations of the Local Density of States in Disordered Photonic Materials. *Phys Rev Lett* 119, 1–6 (2017).
8. Lio, G. E., Nocentini, S., Pattelli, L., Cara, E., Wiersma, D. S., Rührmair, U., & Riboli, F., Quantifying the Sensitivity and Unclonability of Optical Physical Unclonable Functions. *Adv Phot Research*, 2200225 (2022).
9. McGrath, T., Bagci, I. E., Wang, Z. M., Roedig, U. & Young, R. J. A PUF taxonomy. *Appl Phys Rev* 6, 011303 (2019).
10. Gao, Y., Al-sarawi, S. F. & Abbott, D. Physical unclonable functions. *Nature Electr.* 3, 81-91 (2020).
11. Rührmair, U. & Holcomb, D. E. PUFs at a glance. *Proceedings -Design, Automation and Test in Europe, DATE,* 1-6 (2014).
12. Lugli, P. et al., Physical unclonable functions based on crossbar arrays for cryptographic applications. *International Journal of Circuit Theory and Applications* 41, 619–633 (2013).
13. Rührmair, U. et al., Modeling attacks on physical unclonable functions. *Proceedings of the ACM Conference on Computer and Communications Security*, 237–249 (2010).
14. Suh, G.E. and Devadas, S., Physical unclonable functions for device authentication and secret key generation. In Proceedings of the 44th annual design automation conference, 9-14 (2007).
15. Arppe, R. and Sørensen, T.J., Physical unclonable functions generated through chemical methods for anti-counterfeiting. *Nat. Rev. Chem.* 1, 4, 0031(2017).
16. Carro-Temboury, M. R., Arppe, R., Vosch, T. & Sørensen, T. J. An optical authentication system based on imaging of excitation-selected lanthanide luminescence. *Sci. Adv.* 4, (2018).
17. Feng, J., Wen, W., Wei, X., Jiang, X., Cao, M., Wang, X., Zhang, X., Jiang, L. and Wu, Y., Random organic nanolaser arrays for cryptographic primitives. *Adv. Mater.*, 31(36), 1807880 (2019).
18. Leem, J. W. et al. Edible unclonable functions. *Nat. Commun.* 11, (2020).
19. Smith, A. F., Patton, P. & Skrabalak, S. E. Plasmonic Nanoparticles as a Physically Unclonable Function for Responsive Anti-Counterfeit Nanofingerprints. *Adv. Funct. Mater.* 26, 1315–1321 (2016).
20. Yao, W., Lan, R., Li, K. & Zhang, L. Multiple Anti-Counterfeiting Composite Film Based on Cholesteric Liquid Crystal and QD Materials. *ACS Appl. Mater. Interfaces* 13, 1424–1430 (2021).
21. Bin Tarik, F., Famili, A., Lao, Y. & Ryckman, J. D., Robust optical physical unclonable function using disordered photonic integrated circuits. *Nanophotonics* 9, 2817–2828 (2020).
22. Fratalocchi, A., Fleming, A., Conti, C. & De Falco, A., NIST-certified secure key generation via deep learning of physical unclonable functions in silica aerogels. *Frontiers in Optics and Photonics* 471–478 (2021).
23. Di Falco, A., Mazzone, V., Cruz, A. & Fratalocchi, A., Perfect secrecy cryptography via mixing of chaotic waves in irreversible time-varying silicon chips. *Nat. Commun.* 10, 1–10 (2019).
24. Pappu, R., Recht, B., Taylor, J., & Gershenfeld, N. Physical one-way functions. *Science*, 297, 2026-2030 (2002).

25. Horstmeyer, R., Judkewitz, B., Vellekoop, I. M., Assawaworrarit, S. & Yang, C. Physical key-protected one-time pad. Sci Rep 3, 1-6 (2013).
26. Horstmeyer, R., Assawaworrarit, S., Ruhrmair, U. & Yang, C. Physically secure and fully reconfigurable data storage using optical scattering. *Proceedings of the 2015 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2015* 157–162 (2015).
27. Bosworth, B. T. et al., Unclonable photonic keys hardened against machine learning attacks. *APL Photonics* 5, 010803 (2020).
28. Kursawe, K., Sadeghi, A. R., Schellekens, D., Škorić, B. & Tuyls, P., Reconfigurable physical unclonable functions - Enabling technology for tamper-resistant storage. *IEEE International Workshop on Hardware-Oriented Security and Trust, HOST* 2009, 22–29 (2009).
29. John, R. A. et al., Halide perovskite memristors as flexible and reconfigurable physical unclonable functions. *Nat. Commun.* 12, 1-11 (2021).
30. Kim, Y. et al., Reconfigurable Multilevel Optical PUF by Spatiotemporally Programmed Crystallization of Supersaturated Solution. *Adv. Mater.* 2212294 (2023).
31. Gan, Z. et al. Reconfigurable Optical Physical Unclonable Functions Enabled by VO2Nanocrystal Films. *ACS Appl Mater Interfaces* 14, 5785–5796 (2022).
32. Burr, W. E. et al. Electronic Authentication Guideline - NIST Special Publication 800-63-2. 1–123 (2013).
33. Daugman, J. Information theory and the iriscode. *IEEE Transactions on Information Forensics and Security* 11, 400–409 (2016).
34. Daugman, J. The importance of being random: statistical principles of iris recognition. *Pattern Recognit* 36, 279–291 (2003).
35. Guo, S. M. et al. Preparation of a thermally light-transmittance-controllable film from a coexistent system of polymer-dispersed and polymer-stabilized liquid crystals. *ACS Appl Mater Interfaces* 9, 2942–2947 (2017).
36. Da Cunha, M.P., van Thoor, E.A., Debije, M.G., Broer, D.J. and Schenning, A.P., Unravelling the photothermal and photomechanical contributions to actuation of azobenzene-doped liquid crystal polymers in air and water. *Journal of Materials Chemistry C*, *7*(43), pp.13502-13509 (2019).
37. Khoo, I.C. and Wu, S.T., Optics and nonlinear optics of liquid crystals (Vol. 1). World scientific (1993).
38. Dierking, I. Polymer network-stabilized liquid crystals. *Adv Mater* 12, 167–181 (2000).
39. Lee, Y.-H., Gou, F., Peng, F. & Wu, S.-T., Hysteresis-free and submillisecond-response polymer network liquid crystal. *Opt Express* 24, 14793 (2016).
40. Ondris-Crawford, R. et al. Microscope textures of nematic droplets in polymer dispersed liquid crystals. *J Appl Phys* 69, 6380–6386 (1991).
41. Rührmair, U., Hilgers, C. & Urban, S. Optical PUFs Reloaded. *IACR Cryptology* (2013).
42. Uppu, R. et al. Asymmetric cryptography with physical unclonable keys. *Quantum Sci Technol* 4, 1–20 (2019).
43. Barker, E. & Kelsey, J. Recommendation for the Entropy Sources Used for Random Bit Generation, *NIST Special Publication 800-90B* (2012).
44. Vijayakumar, A., Patil, V. C., Prado, C. B. & Kundu, S. Machine learning resistant strong PUF: Possible or a pipe dream? *Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust, HOST* 19–24 (2016).

45. Vijayakumar, A., Patil, V. C., Prado, C. B. & Kundu, S. Machine learning resistant strong PUF: Possible or a pipe dream? Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust, HOST 19–24 (2016).
46. Elbirt, A. J., Yip, W., Chetwynd, B. & Paar, C. An FPGA-based performance evaluation of the AES block cipher candidate algorithm finalists. IEEE Trans Very Large Scale Integr VLSI Syst 9, 545–557 (2001).
47. Škorić, B., Pinkse, P. W. H. & Mosk, A. P. Authenticated communication from quantum readout of PUFs. Quantum Inf Process 16, 1-9 (2017).
48. Goorden, S. A., Horstmann, M., Mosk, A. P., Š, B. & Pinkse, P. W. H. Quantum-secure authentication of a physical unclonable key. *Optica*. 1(6), 421-424 (2014).
49. Eliezer, Y., Ruhrmair, U., Wisiol, N., Bittner, S. and Cao, H.,. Exploiting structural nonlinearity of a reconfigurable multiple-scattering system. arXiv:2208.08906 (2022).
50. Vijayakumar, A., Patil, V. C., Prado, C. B. & Kundu, S. Machine learning resistant strong PUF: Possible or a pipe dream? *Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust, HOST* 19–24 (2016).

Methods

Sample preparation. The preparation of PD&SLC is based on the phase separation and emulsion of a dye-doped LC monomeric mixture and polydimethylsiloxane (PDMS) precursors (elastomer and curing agent in a 10:1 ratio). The chromophore (Dispersed Red 1, DR1, Sigma Aldrich) is the 5% in weight of the LC mesogen (4-Cyano-4'-pentylbiphenyl, 5CB, Sigma Aldrich). The liquid crystalline mixture is the 5% in weight of the PDMS precursors. The stabilized liquid crystal formulation has been obtained by adding a cross-linker (bi-acrylate liquid crystal molecule, RM257 purchased at SYNTHON Chemicals GmbH & Co. KG,Wolfen, Germany) to create a polymeric network into the liquid crystal droplets to facilitate the liquid crystal alignment recovery after the LC phase transition. To this end, the cross-linker has been added in the 4% in weight to the LC mixture and the thermal polymerization of the polymeric backbone was driven by a thermal initiator (AIBN, 1% in weight). After emulsion, the mixture is put under vacuum to remove air bubbles and infiltrated in a glass cell made by two glasses separated by a spacer of 140 μm. After one night under the chemical hood for air degassing, the thermal polymerization and curing was done first in an oven at 80°C for 10 min and then at 100°C for one hour. The scattering properties of the HPUF can be tuned by controlling the concentration of liquid crystal droplets (from 2% to 10% in weight with respect to the transparent PDMS) and the physical thickness of the sample (from 50 to 170 μm). In this way, optical thicknesses in between 0.1 and 2 can be obtained. To further increase the optical thickness, TiO_2 nanoparticles (with diameter of around 100 nm) can be added to PDMS for a TiO_2 doped PD&SLC.

Differential scanning calorimetry (DSC). DSC measurements were performed to carefully determine the nematic to isotropic transition temperature of the dye doped stabilized liquid crystal mixture. The liquid mixture has been studied before the polymerization at a temperature scan rate of 10°C/min starting from 0°C up to 50°C. The sample mass was around 7 mg.

Optical switching of the HPUF. The switching among the PUF levels is achieved by illuminating the hardware with blue incoherent light (L_k^{Trans}) that transforms the internal state of the PUF by absorbing light via the chromophore (DR1) and thereby generating a temperature driven LC phase transition. The local temperature increase induces an unavoidable thermal diffusion process on a length scale that is determined by the thermal diffusion length of the polymeric film, $l = (D * \tau)^{1/2} \simeq 1\ mm$, given the thermal diffusivity of PDMS, $D = 10^{-7}\ m^2/s$, and the sample illumination time τ =20 sec. In order to induce an effective

modulation of the scattering potential, therefore limiting the effect of thermal diffusion, we chose a transformer challenge with 4x4 macro-pixel checkerboard transforming challenge with a macro-pixel size of the order of 1,7 mm. The thermal diffusion reaches a steady state in around 20 seconds when the absorbed energy is equal to the dissipated energy by heat.

Thermal imaging. The spatial and temporal temperature distribution of the HPUF has been monitored along the illumination with the transformer challenge (generated by the projector @470 nm). The thermal camera (7.5-14 μm range, Flir A400) has been placed at 15 cm from the sample whose cover glass has been removed. The polymer emissivity has been calibrated on a hot plate using as reference sample a black tape and tuning the emissivity of the polymer to match the temperature of the reference sample.

Experimental optical apparatus. We exploited the spatial modulation of the beam intensity for the challenge generation. The beam of a Helium-Neon laser (5mW) is expanded and sent collimated on a DMD (Texas instruments, DLPLCR6500EVM) that modulated the light intensity for the challenge generation. The challenge is projected on the PUF with a dimension of 1 cm^2. The configuration beam, made by the LED blue light, made by the projector (Texas Instruments, Lightcrafter 4500, DLPLCR4500EVM) is then overlapped on the same area. Among the RGB color of the projector LED, the blue LED was chosen as it better matches the absorption peak of the dye. Both light sources operate at low continuous wave intensities. The diffused red light is then collected in the far field (20 cm far apart from the sample) by a CCD camera (Apogee Alta, 1600x1200 pixels, 16 bits) and a long pass filter (500 nm) is used in front of the camera to prevent blue light collection. The acquisition time (3Hz) is limited by the integration time of the camera and the mechanical shutter control and they can be improved with others CCD or CMOS cameras. Cross polarizers are inserted before and after the cryptographic primitive to detect only multiple scattered light at the CCD sensor.

Opacity measurement. The opacity that we defined as $\ln (I_{in}/I_{out})$ has been measured by using the Helium-Neon laser also used to characterize the HPUF. The collimated and expanded beam (diameter around 5mm) is then sent to an integrating sphere where both the impinging intensity and the HPUF transmitted intensity have been measured.

POM analysis. To analyze the material behavior at the microscale, polarized optical microscope (POM) images have been recorded to monitor the LC alignment in the different LC phases (Fig. 2d-f). The typical pattern observed at POM reflects the birefringence and the LC nematic director orientation of each droplet: the four dot cross indicates a radial alignment in the nematic phase[40]. When the configuration beam is shined on the sample by the microscope objective (Fig. 2e), a black area appears as the LC ordering is lost and an isotropic phase is attained within the droplets, indicating that the cross-linking network does not prevent the LC disordering to the isotropic phase. Once the blue illumination is removed, the system evolves in around 10 seconds to the previously aligned configuration with the same four dot feature present before the configuration (as highlighted by the green circles of Fig. 2f). This reversible mechanism is enabled in the present formulation whereas polymer dispersed liquid crystals (absence of the cross-linked backbone) do not guarantee a full recovery of the initial alignment.

Gabor Filter. A Gabor filter is a linear filter used in image processing consisting in a Gaussian kernel function modulated by a sinusoidal plane wave. The Gabor transformation extracts the relevant orientation and spatial frequency content of the 2D speckle images that after binarization result in binary keys. In our analysis, we employed the Gabor hashing as one of the most used filters, but other filters that can be empirically optimized to maximize the number of independent bits per each image[1]. The parameters of the Gabor filter have been tuned in order to maximize the extractable entropy of raw responses (the

characterization is reported in Supplementary Fig. 5). In particular, a filter wavelet of 6 pixels and an angle of 45° are used for the analysis of the all the speckle pattern of the PUF described in this work.

FHD analysis and entropy. The fractional Hamming distance (FHD) is the number of bits that differ in a pair of binary keys normalized to the bitstring length. This metric allows to compare in pairs all the responses of a PUF library for evaluating the stability of the responses to a same challenge (*like* FHD distribution) and the independence of the responses to random challenges (*unlike* FHD distribution). In the ideal case, equal keys (*like* keys) are characterized by FHD equal to zero, while different keys (*unlike* keys) have, on average, 50% of bits that disagree (FHD=0.5). The PUF characterization consists in collecting the responses to a set of random challenges (whose number varies in this work in between 100 and 1000) multiple times. The raw speckle patterns are converted into a set of binary strings by using a standard hash function (via a Gabor transformation). All the strings are compared by using the fractional Hamming distance (FHD) as the metric. The *like* FHD distribution has been calculated by comparing the responses (acquired at different times) to the same challenge to monitor the stability of the system. The *unlike* FHD distribution has been calculated by cross-comparing in pairs all the responses of the ensemble. The *unlike* FHD distribution is well approximated by a binomial distribution, in case of quasi-independent responses and presence of a certain degree of correlation among the keys. In the limit of a large number of degrees of freedom, the discrete binomial distribution can be approximated with a Gaussian function. The width and spreading of the distribution provide information about the degree of correlations between the bit sequences generated by different challenges. By assuming that the unlike FHD can be modeled with an equivalent binomial distribution $B(N,p)$ that in the limit of large number of degrees of freedom can be fitted by a Gaussian function, the number of the independent bits N – that correspond to the number of independent degrees of freedom – of the equivalent Bernoulli process can be expressed as a function of the mean value p and variance o^2 of the distribution, $N = \frac{p*(1-p)}{\sigma^2}$ [24,33] . Given the total length of N_{tot} =7056 bits of the binary strings that we extract from the raw speckle pattern, the number of bits of information is $N=N_{tot}*H$ where H is the entropy per symbol (bit) [2]. Other security metrics can be adopted to measure the PUF entropy such as standard error, Pearson correlation coefficient, and mutual information. The number of independent bits N of the keys[24,33], that are a measure of the PUF resilience and security against cyber-attacks, relates to the response uniqueness[3], encoding capacity of the PUF[15] and to the number of independent pairs of challenge/response[4].

Considering a HPUF with K independent levels each one with an entropy of 2^N, the total complexity and encoding capacity is $\approx 2^{N*log_2 K} = 2^{lo\ _2 K^N} = K^N$, with N being a large number. In this case, the complexity has a polynomial growth with the number of levels, and the exponent of the polynomial N is also extremely large, so the growth in complexity is a significant one (much more than linear).

Optical PUF characterization. The characterization of the one-single level PUF is done by interrogating the HPUF with challenges (C_i^{Probe}, L^{Trans}=0) with i={1,…,100}. The challenge-response characterization of a two-level HPUF is done by illuminating each level with the same set of 100 random challenges (Fig. 3d). The unlike FHD distribution is obtained by comparing all possible pairs of responses (roughly 2*104 pairwise comparisons), while the like FHD distribution is obtained by comparing a defined set of 150 random challenges acquired multiple times for each level. The characterization of the ten level PUF has been done by first defining a set of 10 transformer challenges (L_k^{Trans}, with k={1,..,10}) by choosing 10 elements of the Walsh-Hadamard binary basis as a subset of a complete 16 orthogonal set of 4x4 macropixel images. Each level is then interrogated with the same set of randomly selected challenges C_i^{Probe} with i={1,.., 100} and all the 1000 responses R_{ik}, with i={1,.., 100} and k={1,.., 10} collected. The CRP library gor the 10 level HPUF is available (https://doi.org/10.5281/zenodo.8377156).

Equivalent Markov Model. Binary Markov chains are a classical stochastic model used to model pseudo-randomly changing binary sequences, in which the bit correlations are described by the symbol transition probabilities. For a binary sequence (with states 0 and 1), the transition matrix is $(\alpha, 1-\alpha, 1-\beta, \beta)$ where α (β) is the permanence probability of the "0"("1") state and 1-α (1-β) is the transition probability. Random binary keys are characterized by α=β=0.5. Equivalent Markov chains that reproduce the statistical properties of the binary keys extracted from the HPUF are characterized by a symmetric transition matrix wherein the transition probabilities between zeros and ones are identical (α=β). The equivalent Markov chain model allows the estimation of the entropic content and the study the statistical properties of the HPUF keys. In this work, the coefficients of the transition matrix of the Markov model (α,β) have been adjusted in order to generate bit strings whose FHDs well reproduce the FHD histogram calculated from experimental data. The entropy rate of the Markov chains has been calculated analytically: $H = \pi(0) * [-\alpha * log\ \alpha - (1-\alpha) * log\ (1-\alpha)] + \pi(1) * [-\beta * log\ \beta - (1-\beta) * log\ (1-\beta)]$[5] with $\pi(0) = \frac{\alpha}{\alpha+\beta}$ and $\pi(1) = \frac{\beta}{\alpha+\beta}$. In case of symmetric MC, the entropy can be simplified and expressed as a function of the permanence probability $\alpha : H = [-\alpha * log\ \alpha - (1-\alpha) * log\ (1-\alpha)]$. For a first-order Markov chain, the probability of each bit value in the binary string depends only on its predecessor. However, this induces a non-zero correlation between *X(n)* and *X(n+d),* where n is the position of the bit in the string and d is the distance or lag in bits, when *d* is greater than 1. We performed a correlation analysis of the bits of the equivalent Markov chains at different "lags" for different HPUF composed by a number of levels that varies in between two and ten (Fig. 5c). The correlation between *X(n)* and *X(n + d)* of the equivalent Markov chain decreases as a function of the number of cumulated levels and reaches its minimum when roughly ten levels are cumulated.

Data Availability

Data supporting the findings in the present work are available in the Article or its Supplementary Information. Additional data are available from the corresponding authors upon request or available via Zenodo at https://doi.org/10.5281/zenodo.8377156.

Methods-only references

[1] Rührmair, U., Hilgers, C. & Urban, S. Optical PUFs Reloaded. IACR Cryptology (2013).

[2] Cover, T. M. & Thomas, J. Chapter 2. Entropy, Relative Entropy and Mutual Information. Entropy vol. 1 (1991).

[3] Scholz, A. et al., Hybrid low-voltage physical unclonable function based on inkjet-printed metal-oxide transistors. Nat Commun. 11, (2020).

[4] Tuyls, P., Škorić, B., Stallinga, S., Akkermans, A. H. M. & Ophey, W., Information-theoretic security analysis of physical uncloneable functions. Lecture Notes in Computer Science 3570, 141–155 (2005).

[5] Arppe-Tabbara, R., Tabbara, M. & Sørensen, T. J. Versatile and Validated Optical Authentication System Based on Physical Unclonable Functions. ACS Appl Mater Interfaces 11, 6475–6482 (2019).