Recent Advances in Photonic Physical Unclonable Functions

Fabio Pavanello, Ian O'Connor
Univ Lyon, CNRS, ECL, INSA Lyon, UCBL, CPE Lyon, INL, UMR5270
Écully, France
fabio.pavanello@ec-lyon.fr

Ulrich Rührmair
Physics Department, LMU Munich, Germany
ECE Department, U of Connecticut, USA
Munich, Germany – Storrs, CT, USA
ruehrmair@ilo.de

Amy C. Foster
Dept. of Electrical and Computer Engineering
Johns Hopkins University
Baltimore (MD), USA
amy.foster@jhu.edu

Dimitris Syvridis
Dept. of Informatics and Telecommunications
University of Athens
Athens, Greece
dsyvridi@di.uoa.gr

Abstract

This special session paper discusses recent advances on photonic physical unclonable functions (PUFs), providing a broader overview of and motivation for photonic PUFs. We discuss their potential advantages, such as a higher entropy, larger complexity, and possibly better resilience against machine learning attacks. We also deal with some recent implementations based on linear and non-linear optics, alongside with their main advantages and limitations.

1 Photonic PUFs: An Introduction

Fabio Pavanello, Ian O'Connor, Ulrich Rührmair

A. Motivation and Overview

Security applications and protocols are an integral part of our modern digital society. They play a tacit, but indispensable role in many of our daily routines, such as the exchange of sensitive data in communications, banking, or medical records, or the protection of electronic hardware and pharmaceutical products against counterfeiting [1], [2]. In this situation, the significant increase in interconnected devices within the Internet of Things (IoT), estimated to reach nearly 30 billions by 2023 in a Cisco internal report [3], poses a qualitatively new and unprecedented security challenge to the security community. It calls for new types of protection measures that can maintain security and privacy on large scales even in the vicious threat landscape of the IoT.

One central and still unresolved issue consists of safely storing digital secret keys in the mobile, highly connected, and lightweight devices that are typical for the IoT. In traditional, digital approaches, these keys are inevitably required to encrypt and protect sensitive information, or to enable secure authentication over digital communication lines [4]. In many circumstances, however, they may be extracted by sophisticated adversarial attacks, including side channels or invasive methods. Most recently, powerful attack vectors at a processor level, such as Spectre and Meltdown, have even demonstrated that any given memory sector, e.g., storing secret keys or passwords, may be accessed by an attacker *under certain circumstances* [5], [6].

To circumvent these and similar issues, Physical Unclonable Functions (PUFs) were introduced in two separate and independent research strands by Pappu et al. [7] and Gassend et al. [8] around two decades ago. In a nutshell, a PUF is a randomly disordered, unique, and unclonable physical system that implements a potentially (slightly) noisy, but otherwise deterministic function. This function maps a given PUF-input (or *"challenge"*) to a PUF-output (or *"response"*). The function shall differ from PUF to PUF, since uncontrollable fabrication variations and mismatches make every PUF (and its challenge-response behavior) unique.

The main characteristic properties expected from a PUF are as follows (compare [9]–[11]):

- *Physical Uniqueness:* Due to its random manufacturing variations, every PUF is unique and differs from every other PUF. This *physical* uniqueness also leads to a *digital* uniqueness on the level of a PUF's numeric challenge-response pairs (CRPs): A sufficient number of CRPs can uniquely identify every PUF, comparable to a human fingerprint.
- *Physical Unclonability:* A PUF cannot be physically cloned, not even by active and well-equipped adversaries. This is due to the current limitations in the precision of existing manufacturing technologies; with new, future technologies, this fact may change. It needs to be assessed anew for each PUF design.
- *Digital Unpredictability:* It shall be impossible to numeri-

cally predict (for example via simulations, or via machine learning algorithms, etc.) unknown CRPs of a PUF. This impossibility shall hold even if the adversary knows many other CRPs of the same PUF, and/or arbitrary CRPs of other PUFs with the same design or from the same fabrication series.
- *Reliability:* The CRPs of a PUF usually shall be reasonably stable over time and against environmental variations. At least after suitable error correction, it shall be possible to regard the behaviour of the PUF as a (noisy) function, justifying the name *"PUF"*. Depending on the exact application, either perfect error correction is necessary (e.g., if a system-internal secret key is derived from a PUF's responses). Sometimes also certain levels of response noise can be tolerated by introducing simple error margins (e.g., in classical CRP-based remote identification protocols via PUFs [7]).
- *Reasonable Costs and Efficiency:* The PUF shall be efficiently manufacturable and measurable. Low fabrication and testing costs, as well as integration and electrical driving feasibility within CMOS-based circuitry, are helpful properties for their widespread deployment.

We would like to stress that uniqueness and unclonability are two different properties, which do not necessarily imply each other: As a first example, think of a classical digital identifier, which is obviously unique, but not unclonable. Or, secondly, of a physical structure that is unique on lengthscales that are so large that they can be reproduced by latest fabrication methods. Both examples illustrate that uniqueness does not imply unclonability. Exemplary structures that are (at least hoped to be) unclonable for adversaries, but which are not unique in the above sense, include holograms or the security features of banknotes. Interested readers are encouraged to come up with further examples that differentiate uniqueness and unclonability by themselves.

Our above list conveniently summarizes the main features any PUF should possess in everyday language. Its seeming simplicity should not hide two facts, though: First of all, a vast amount of different PUF-subtypes exists in the literature, each of them possessing their own additional features targeted for certain application scenarios. While our list tries to capture the "essence" of PUFs, which all subtypes have in common, each subtype possesses its own extra features. Characterizing all existing PUF-subtypes is worthwhile, but beyond the scope of this brief introduction. Popular choices include Weak PUFs and Strong PUFs, Controlled PUFs, Erasable PUFs, SHIC PUFs, Unique Objects, Public PUFs and SIMPL Systems, etc., which together populate the entire *"PUF-zoo"*.

We feel that it is important, perhaps even essential for thorough PUF-publications to specify which exact PUF-type the authors are trying to implement; unfortunately, this is not always common practice yet. A second fact we would like to emphasize is that the exact, mathematically rigorous definition of all given PUF-features is unexpectedly complex, and still subject to ongoing work. Readers interested in further details are referred to some of the existing surveys on PUFs, for example [9]–[11], and references therein.

For now, and for the limited purposes of this manuscript, let us just quickly and informally define Weak and Strong PUFs before proceeding (compare again [9]–[11]):

- A *Weak PUF* fulfills the above list of features, but has two additional properties: Firstly, it only has a very small number of challenges per PUF — in the most common case just a single, fixed challenge. Secondly, a Weak PUF is assumed to possess a *"protected"* challenge-response mechanism: Once a Weak PUF (or the device embedding the Weak PUF) has been manufactured and issued to the field, no external parties or adversaries shall be able to access the Weak PUF's responses.
- *Strong PUFs* also meet the earlier list of features, but are characterized by three *other* additional properties: Firstly, they possess very many challenges and thus very many CRPs, too many to read out all of them in feasible time. Secondly, their challenge-response behavior shall be highly complex. Unknown CRPs shall be hard to predict numerically by adversaries, even it they know substantial numbers of other CRPs of the same PUF. Thirdly, the CRP-mechanism or CRP-interface of a Strong PUF can be accessed unrestrictedly by everyone who has access to the Strong PUF (or to the hardware embedding it).

While Weak PUFs are usually confined to use as chip-internal source of secret keys and randomness, Strong PUFs can accomplish slightly more: They can also be employed in more advanced cryptographic protocols, such as identification, key exchange, or oblivious transfer. Again, we refer to the abovementioned surveys [9]–[11] for further reading.

B. Main Vulnerability of Electronic Strong PUFs: Numeric Modeling Attacks

Although one of their historically first implementations was of optical nature [7], PUFs to this day have received much stronger attention within the circuit community than among optics researchers. Most of these modern electronic PUFs are implemented in CMOS, sometimes building on architectures inspired by the field of digital electronics [12]. They are frequently realized on reconfigurable platforms like FPGAs, which are widespread, flexible, and easily available to security researchers. Popular examples include SRAM PUFs [13], [14], ring oscillator PUFs [15], bistable ring PUFs [16], and, of course, arbiter PUFs [8], [15], just to cite the most common ones. Design-wise, these PUFs rely on the random character of their 1/0 cell states at power-up (SRAM PUFs), or on their signal delays, where small fluctuations from the nominal switching time or signal propagation time can be measured and converted into PUF-responses (ring oscillator, bistable ring, and arbiter PUFs).

There is one major drawback of modern electronic Strong PUFs, however: Many of them can be attacked efficiently by so-called *"modeling attacks"*. These attacks can, at least in principle, take two basic forms:

- *Basic Modeling Attacks on Strong PUFs:* In the most simple and basic form of a modeling attack, a com-

parably small subset of the CRPs of a given Strong PUF is collected. This subset is used as training set for a machine learning (ML) algorithm. If the learning phase is successful, the ML-algorithm and its trained model can numerically predict the attacked PUF with high accuracy. Such a successfully trained ML-model is sometimes called a *"digital clone"* of the PUF.
Most existing modeling attacks on electronic Strong PUFs assume that the adversary knows the basic circuit design of the attacked PUF, and that only the individual manufacturing variations are unknown to him. These variations (or the circuit parameters influenced by them) must be then derived by the used ML-algorithm from the collected CRP data. This attack model appears reasonable in practice, since adversaries could obtain many PUFs from the same series, invasively (and potentially destructively) inspect them to learn their designs, and then attack other PUFs from the same series.

- *Modeling Attacks with Additional Side-Channel Information:* In a more advanced form of Strong PUF modeling, additional information besides the mere, digital CRP-values yet further improves ML-performance. For example, the stability of PUF-CRPs (i.e., the noise/bit flips in their responses when the same challenge is applied multiple times) can provide highly valuable information to the adversary. For certain architectures, such as the well-known XOR Arbiter PUF, it can boost state-of-the-art ML-performance from exponential to polynomial. The same applies to the power consumption (or other parameters) of a PUF-circuit during its operation: If combined with suitable ML, it can create polynomially efficient ML-attacks for PUFs that without side channels would seem exponentially hard to machine learn. Again, one prominent example for this effect is the XOR Arbiter PUF [17], [18].

Unfortunately, modeling attacks have proven incredibly effective on electronic Strong PUFs in the past (see, e.g., [18]–[20]). Very few architectures (if any) have remained beyond their reach. One of them are Strong PUFs with super-high information content, so-called *"SHIC PUFs"* [21]. They possess provable security against modeling, as all their CRPs are information-theoretically independent. However, SHIC PUFs have the intrinsic drawback of relatively slow read-out speeds and large area consumption of around 1cm^2. In sum, the realization of secure and efficient electronic Strong PUFs still remains a major open challenge to the PUF-community.

C. The Promise of Photonic PUFs: Boosted Complexity, Enhanced Reliability, and ML-Resilience

There are good reasons to believe that photonic PUFs might finally bring about the technology for implementing secure, highly complex, yet fast and stable Strong PUFs *in silicon*. Compared to electronic PUFs, photonic PUFs offer a much richer physics to exploit and can allow to achieve highly complex mixing of signals aside their analog propagation, in particular if non-linear phenomena are exploited [22]. These aspects are key to their superior performance against ML attacks which can predict the behavior of standard implementations of electronic PUFs e.g., XOR arbiter, with better than 99% accuracy [23].

In fact, even configurations analogous to the one initially proposed by Pappu *et al.* have experimentally shown a large degree of robustness against this type of attacks. Such pioneering configuration was based on a matrix of dispersed scattering microspheres. A laser beam impinging on the PUF's surface and located at a well-defined position with respect to the PUF allowed to obtain a complex diffraction pattern (or *speckle*) recorded at a given distance onto a CCD camera sensor. The robustness of this approach against ML attacks is due primarily to the complex speckle response and to the very large parameter space, up to 2.37×10^{10} uncorrelated challenges were reported for the original photonic PUF configuration [24], [25].

However, such configuration can be seen as a collection of spatially isolated PUFs, defined by the laser position with respect to the PUF surface, and therefore it does achieve enhanced security at the expenses of device dimensions, testing complexity and subsequent reduced reliability (highly sensitive to laser/PUF alignment) as well as increased costs due to its lack of integration capability with CMOS circuitry.

Although various approaches exist to reduce device dimensions, without affecting the internal complexity of the PUF by e.g., using laser beams with different diameters and optimized microsphere dimensions, the improvement factor does not allow to shrink the dimensions by several orders of magnitude for compact integration [24]. To enhance their reliability, alternative transformations to the one originally used (Gabor transformation) after speckle acquisition have been also proposed [24]. However, these solutions are not considered sufficient to bring strong photonic PUFs ubiquitous in the IoT market.

These obstacles reflect the main reasons why photonic PUFs have not followed the same path of their electronic counterparts. However, recent work has demonstrated that it is possible to build photonic PUFs integrated in CMOS-compatible platforms and, at the same time, robust against ML and side-channel attacks by e.g., exploiting multiple non-linear optics phenomena such as free carrier absorption and Kerr effect within a chaotic microcavity [22]. The role of non-linearities was clearly demonstrated in [22] where increased optical input powers led to larger errors in response prediction by advanced state-of-the-art deep neural network modeling of the PUF behavior. However, it was also shown that the introduction of non-linearities was not impacting the temporal stability and reliability of the system thanks to its high level of integration.

Integrated photonics based on CMOS-compatible platforms is thus believed to be the principal route towards a scalable and large-scale use of photonic PUFs because of their enhanced compactness, reduced cost and superior reliability compared to bulk optics approaches as well as to electronic approaches based on transistors which strongly suffer from aging issues

and thermal fluctuations and for which heavy use of error correction codes is needed, not always a viable solution in terms of energy consumption and cost, especially for IoT devices. Besides, monolithic integration of photonics with electronics can further allow to achieve modules with high performance in terms of energy consumption, integration density and speed, up to 32 nm CMOS nodes. [26], [27]. Out of the different photonic platforms that have been considered, SOI and SiNOI are those that have received most attention thus far due to their current level of maturity and accessibility for scalable, large-volume fabrication [28]–[31]. SOI platforms offer additional advantages compared to standard SiNOI platforms such as the possibility to have active devices e.g., modulators and detectors, directly integrated without the need for hybrid integration approaches [32]. Integration of these key components is an important asset for reliability and cost reasons. PUFs built in integrated photonics platforms have a much stronger resilience to aging effects (typical in transistors) which are a major source of issues in electronic PUFs and require heavy use of error correction codes.

2 Physical Keys in Silicon Photonics

Amy C. Foster

Modern secure communications and authentication suffer from formidable threats arising from the potential for copying of secret keys stored in digital media. To address this vulnerability, a class of cryptographic devices known as physical unclonable functions (PUFs) are being developed. A user derives a digital key from a PUF's physical behavior, which is sensitive to physical idiosyncrasies that are beyond fabrication tolerances and thus a PUF cannot be duplicated. Electronic approaches offer the compatibility of integrating PUFs monolithically with the hardware system and many such devices have been proven as "strong PUFs" indicating the information content in the device is large. However, machine learning (ML) attacks have been successful at breaking even strong electronic PUFs. Due to the rich nature of light and its interactions with media, optical approaches to PUFs result in inherently "strong" devices with a great deal of information content. Optical approaches have shown resistance to ML attacks, however many such approaches rely on free-space optical components and camera-based detection, therefore making them challenging to package with electronics.

Figure 1 offers a qualitative perspective on the relative strength and practicality of such Electronic and Optical PUFs demonstrating the tradeoff that exists between security and practicality.

The field of integrated silicon photonics involves making optical devices utilizing CMOS electronics fabrication, enabling the integration of photonic/electronic devices onto the same integrated chip, and offers a natural route to overcoming the tradeoff between security and practicality for strong PUFs.

Nonlinear silicon-based photonic PUFs are designed to strike a balance between the tremendous security offered by optical keys and the electronic compatibility of CMOS circuits. Such devices are compatible with both planar semiconductor fabrication approaches used for CMOS electronics and optical communications hardware. A typical silicon PUF consists of a planar chamfered micro-disk cavity on the order of 30-μm in diameter and 250 nm in height [28] as shown in Fig. 2. Small variations in the device geometry that occur during fabrication coupled with the reverberant ray chaotic cavity design provide the desired properties of unclonability and unpredictability. To "read" the devices, light from a telecommunications laser source is coupled to and from the chaotic optical micro-cavity using robust single-mode waveguides formed in the same layer as the PUF, and standard telecommunications hardware is used to receive and process the response. Notably, the chamfered design permits coupling between the input/output waveguides and several hundred transient spatial modes inside the resonator.

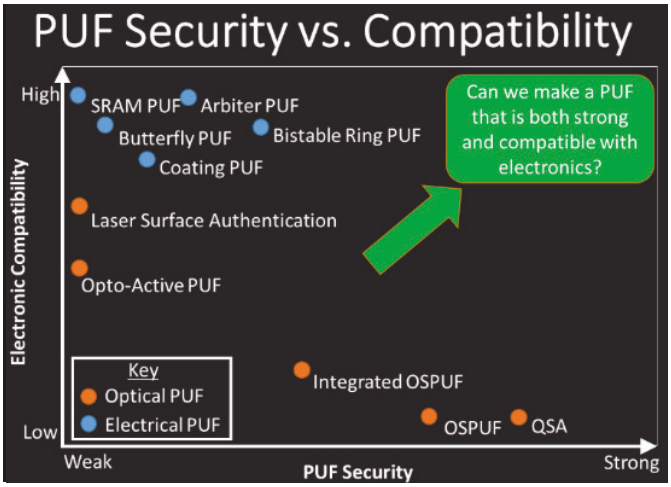

Fig. 1: Qualitative perspective on relative strength and practicality of electronic and optical PUFs

Additional richness of complexity arises when the nonlinear optical properties of the silicon-based materials are exploited, including Kerr effects, Raman scattering, two- and three-photon absorption, and effects from free-carriers. We have demonstrated nonlinear silicon-based photonic PUFs in both single-crystal silicon (c-Si) films as well as hydrogenated amorphous silicon (a-Si:H) films. Due to their beneficial linear

and nonlinear optical properties and chaotic design, both platforms have provided highly unclonable, unpredictable, and ML-attack resistant PUFs. a-Si:H devices provide additional flexibility during fabrication due to the low-temperature deposition of the films and the potential for additional information content due to the random nature of the amorphous film.

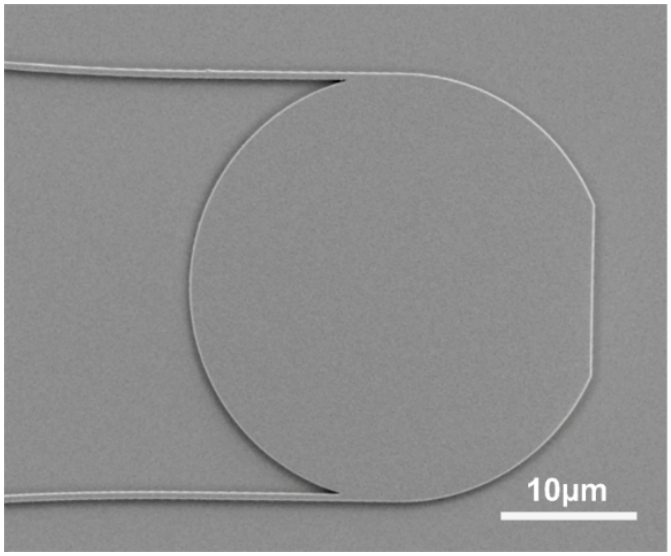

Fig. 2: SEM image of a silicon-based photonic PUF device consisting of a reverberant ray chaotic cavity accessed through robust, single-mode waveguides formed in the same layer as the photonic PUF.

The integrated photonic PUF devices derive their large information content from both the chaotic nature of the cavity as well as the nonlinear optical interactions that occur within the cavity. As we have shown [33], the nonlinearity provides a complex mapping function between the spectro-temporal input to the output of the system, rather than a simple transmission matrix that would be provided through a simple linear system (Fig. 3). This results in information content upper bound potentially on the order of exabits for such a device.

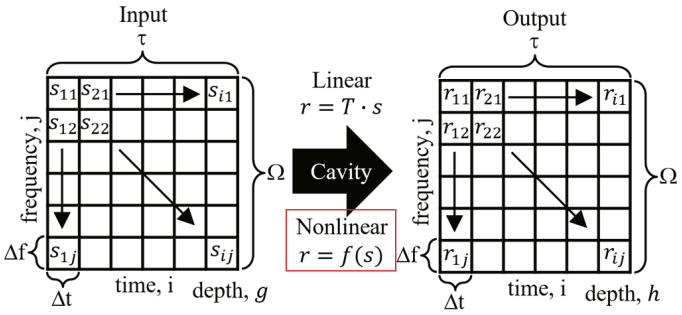

Fig. 3: The nonlinearity provides a complex mapping function between the spectro-temporal input to the output of the system, rather than a simple transmission matrix that would be provided through a simple linear system.

We have performed extensive studies of unclonability in two separate silicon based platforms. In c-SI, we have characterized 12 precise copies (referred to as clones) of a c-Si microcavity, all produced on the same wafer during the same fabrication run [22]. In a-Si:H devices, we have characterized 10 precise copies of an a-Si:H micro-cavity [34]. To test the unclonability of our devices, we apply the same input challenge sequence to exact copies of the same device and compare the resulting photonic PUF responses. The fractional Hamming distance (FHD) between a device and its expected response is considered a "like" distribution, while the FHD between a device and its clone's expected responses are the "unlike" distributions. As shown in Fig. 4, FHD measurements in both platforms show clear separation between each device's response compared to all other clones, also demonstrating unclonability with the existing fabrication techniques. Interestingly, the a-Si:H device outperform the c-Si with regard to reproducibility (low FHD for a given device compared to its own challenge-response library) due to overall better insertion losses resulting in higher SNR.

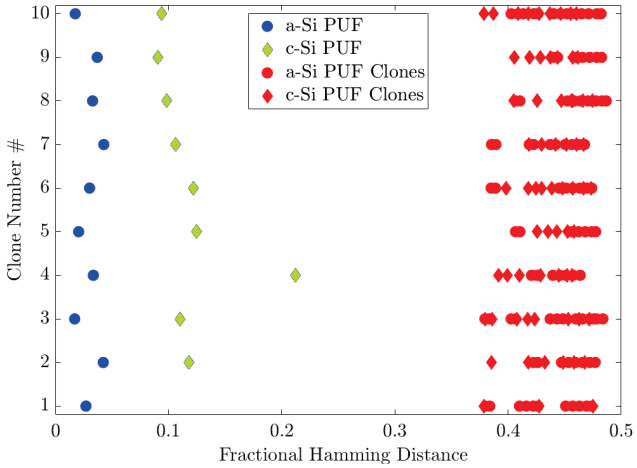

Fig. 4: Fractional Hamming Distance (FHD) for 10 clones in each of two silicon-based platforms: c-Si and a-Si:H.

To quantify the difference in performance between the crystalline silicon (c-Si) and amorphous silicon (a-Si:H) photonic PUFs, we have defined a "Performance Quality Factor," Q:

$$Q = \frac{\mu_{inter} - \mu_{intra}}{\sigma_{inter} + \sigma_{intra}} \quad (1)$$

This quality factor calculates the difference in the means of the like and unlike distributions and divides this value by the sum of the standard deviations of the two distributions. This quality factor is calculated as 8.8 for our crystalline silicon devices, and is slightly larger at 11.08 for the amorphous silicon PUFs (see Fig. 5), indicating what can be interpreted as superior performance. Notably, both platforms demonstrated extremely promising results with large numbers of clones with respect to unclonability.

Successful Machine Learning (ML) attacks can compromise the security of a PUF, as once the challenge response behavior is learned, the full challenge response library can be generated and a PUF device can be spoofed at any time. It is essential that PUFs provide resistance to such attacks. Through both our c-Si and a-Si:H platforms, we have explored our PUF devices' resistance to a variety of ML attacks.

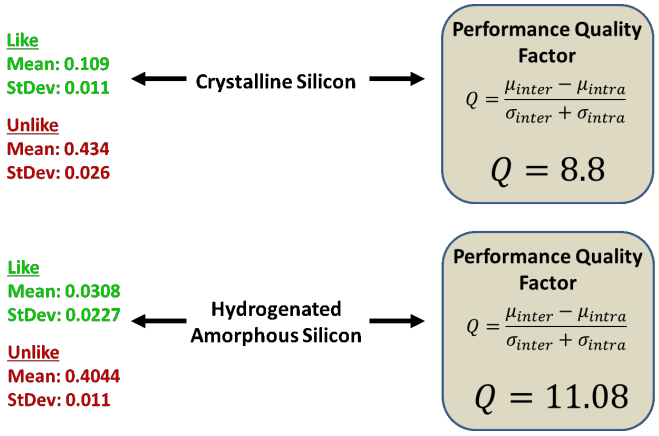

Fig. 5: Summary of the means and standard deviations of the "like" and "unlike" FHD distributions of both material platforms. Also shown is the calculation of a performance quality factor indicating what can be interpreted as superior performance in the a-Si:H devices.

Both direct and side-channel attacks in our c-Si devices [22] with deep neural networks (DNNs) demonstrate our c-Si PUF's resistance to ML with the DNN's ability to learn the device plateauing at all operational power levels. Interestingly, as pulse energy is increased and more optical nonlinearity is experienced, the separation between the FHD of the ML model and the device increases more. To quantify, we have demonstrated False acceptance and false rejection rates at 10^{-22} with pulse energies of 0.36 nJ (and decreasing even further to 10^{-27} when the pulse energies are increased to 1.7 nJ).

The nonlinearity in our a-Si:H devices is an order of magnitude higher than the c-Si platform, and as a result, such devices perform as good as, or better than, c-Si devices with regard to resistance to ML attacks. Figure 6 shows an example ML attack against our a-Si:H devices, where the opening in the two curves represents the difference in accuracy of the ML models to predict the bits of the key as compared to the repeatability of the experimentally validated device. We observe that as the pulse energy increases, the opening between the curves also increases, emphasizing the importance of the optical nonlinearity of the PUF device. Notably, the resistance to ML attacks is occurring with 2-3 orders of magnitude less pulse energy for the a-Si:H devices compared to the c-Si devices.

Through our investigations, we have demonstrated that silicon photonic PUFs possess strong reliability, unclonability, information capacity, and resistance to state-of-the-art ML attacks. In particular, the complex nonlinear optical behavior of the silicon photonic PUFs represents a significant step forward in ML resistance of practical, CMOS compatible PUFs. Whereas linear PUFs, especially electronic PUFs, can be predicted with 99% accuracy under similar ML attacks, the photonic PUF resists this style of attack even at low input powers and it becomes especially resistant at higher optical powers that excite more optical nonlinearities in the cavity.

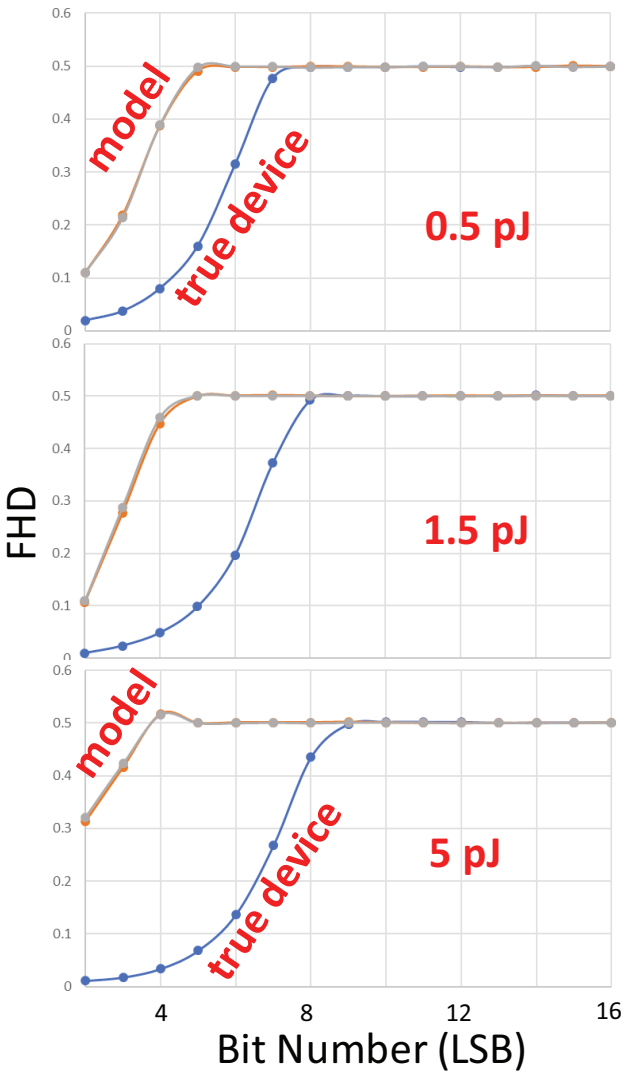

Fig. 6: ML results on the a-Si:H PUF devices for three pulse energies. The opening between the modeling curve and the true device increases as a function of increased pulse energy, demonstrating the importance of nonlinearity on the resistance to ML attacks.

Based on our results, the optical nonlinearity is clearly shown to have critical importance in the resistance of silicon photonic PUFs to such ML attacks. The combination of device robustness and ML attack resistance demonstrated here is unique amongst presently available PUF designs and is critical for applications in hardware and information security. With the recent emergence of silicon photonic foundries and greater adoption of silicon photonics in the microelectronic ecosystem we anticipate that silicon photonic PUFs will provide an ideal hardware security device for future information systems.

3 Photonic PUFs based on speckle image from disordered random optical media

Dimitris Syvridis

As already discussed in the previous sections, random physical structures are very promising means to serve as a root of trust for various cryptographic primitives such as authentication and encryption keys. In fact, and taking into account the asymmetric cryptography related issues (prone to stealth stealing the secret key, delays due to heavy processing requirements, unproven mathematical assumptions, and most importantly quantum computing developments), physical unclonable functions could be the successor technology provided that they satisfy to a large degree the ideal PUF requirements, i.e. deterministic (time invariant operation), support of very large number of challenge response pairs, resistance to machine learning / brute force attacks, unclonability, and of course, real time on demand operation (no digital storage).

The schematic of a typical photonic PUF based on optical speckle recording is shown in Fig. 7. The key part is the random optical medium. Its properties and structure in general dictate the other two critical parts of the PUF, namely the interrogation unit operation principle and architecture and the mathematical algorithms for processing and key extraction.

When firstly proposed by Pappu *et al.* [25], the random medium was a bulk optical scattering unit. The same approach has been in principle followed by other groups e.g., [24]) where the random token was a bulk scattering material combined in some cases with random surface formation.

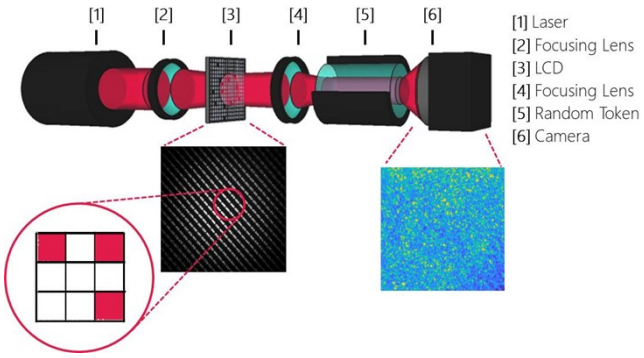

Fig. 7: Schematic of an optical speckle based PUF with the main building blocks been indicated. The laser beam is transmitted through the LCD screen which converts the digital challenge to special light structure illuminating the random optical token. The optical speckle generated at the output is recorded by the camera.

This approach provides sufficiently complex speckle patterns when interacting with a coherent optical beam (e.g. laser diode emission). Combined with space encoded optical inputs, corresponding to different numerical challenges, has the potential of generating highly uncorrelated optical speckle patterns which after proper numerical processing lead to the corresponding numerical responses. Major concern in this case is the maximum number of uncorrelated optical patterns projected to the random medium which result in strongly uncorrelated speckles and in consequence different digital random sequences (keys). This PUF property can be used for true random number generation [35]. Other input parameters could also be used in order to increase the number of challenge response pairs (increase the strength of the PUF) such as laser wavelength.

One of the major criticisms that this type of token has received is its inherent linear behavior. Indeed, scattering is a linear process although at the system level this is not absolutely true in the sense that optoelectronic conversion of the imaging device is governed by the square law. In any case focusing on the linearity of the scattering mechanism, this has two major consequences.

The first is related to the possibility of measuring the transfer matrix experimentally and therefore implement a computational copy of the PUF by numerically modelling this medium. Indeed, such activities have been reported but and successfully determined this transfer matrix of such medium [36], [37]. Unfortunately, this has been achieved for extremely small sizes (illumination areas A) and small thickness d of the disordered medium, e.g. in [5] $A = 18 \times 18$ μm^2 and $d = 10.5$ μm^2. The reason is the number of modes N which depends on the surface according to the relation $N = 2\pi A/\lambda^2$ for the two orthogonal polarizations and the intrinsic correlations between the modes which result in an overall transfer matrix much larger than that obtained by the number of the illuminated elements. Needless to mention that in a typical PUF implementation the area of each of the illuminated elements is in the order some mm^2 and the illumination matrix is in the order of e.g. 128 $\times$ 128 elements. Therefore and even assuming that the intruder has the possibility to remove the random token from its PUF packaging – which is practically impossible without radically modifying the overall PUF properties – the experimental extraction of its transfer matrix is unrealistic.

The second refers to the efficiency of the machine learning attacks. The idea here is to extract the transfer function of the disordered medium using machine learning techniques. In such a case, the potential eavesdropper needs to have direct access to the optical encoding hardware and to the acquisition raw output. This is not obvious for a practical implementation since apart from the proper electro-mechanical assembly, the complete system should operate in secure execution environment. In any case, it is still interesting to see whether the scattering process can be modelled with machine learning. There are quite some works recently focusing on this topic. For example, in [38] the authors develop and demonstrate a Convolutional

Neural Network (CNN) able to learn the statistical information contained in the speckle intensity patterns captured on a set of diffusers having the same macroscopic parameter. They use the trained CNN to make high quality object predictions through a different set of diffusers on the same class. A similar approach is reported in [39] based also on a variant of CNN.

Common characteristic in all these approaches is the reconstruction of well defined images like characters or number figures but not highly complex patterns such as those used to optically encode the numerical challenge in a PUF. Moreover, all these approaches reconstruct the input image from the speckle pattern. According to the PUF terminology they reconstruct the challenge from the response, which is not the desirable action, since what is needed is to reconstruct the response (speckle) from the challenge (transmitted through a public channel). In any case, it should be pointed out that even if the speckle could be reconstructed from the complex structured light image, which has not been achieved up to now, the challenge-response pairs generated by the PUF depend on so many structural, functional and processing parameters in addition to the transfer function of the random token that it would be impossible for someone to disassemble the unit, extract the random token, determine its transfer function and reassemble it as an exact replica of the initial PUF.

An alternative to the bulk optic random token has been proposed in [40], adopting a combination of strongly multimode optical waveguide with scattering facets.

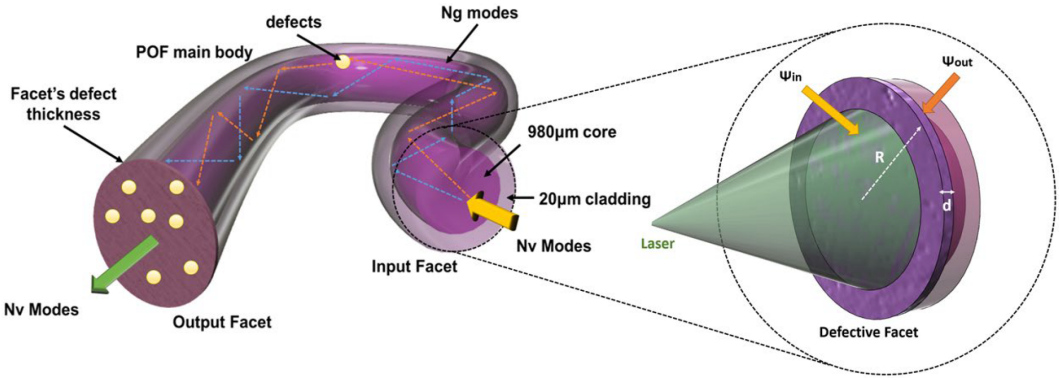

Fig. 8: Schematic of the proposed PUF implementation in [40], presenting the physical mechanisms associated with response generation. Inset depicting the rough fiber's facet, R and d correspond to the radius of the facet and to the average defect size. in and out are related to the initial excited and filtered modes, due to the core-cladding of the fiber and Nv, Ng are the number of modes supported by the facet and the waveguide.

This implementation relies on large core (900 μm) step index polymer optical fiber with facets incorporating randomly induced surface roughness. One of the facets is illuminated by a laser beam and the optical output generates the speckle image recorded by the camera. The challenge in this case is the laser wavelength. The basic mechanisms involved in this type of token are the multimodal behaviour of the fiber, the excitation of a large number of supported modes by the randomly micro structured rough surfaces and the corresponding mode mixing within the waveguide core combined with the scattering from the material imperfections.

Major advantage of the proposed method relative to the conventional bulk tokens is its superiority in terms of the unclonability and the reconfiguration possibility using the same hardware, resulting in a totally different PUF device. Apart from the conventional disordered scattering media, a lot of effort has been put recently for the development of novel tokens using alternative materials, passive or active (e.g. fluorescent, optically pumped quantum dots, etc.). For example in [41] perovskite quantum dot nanostructures are used to produce unclonable fluorescent speckles resulting at the diffraction limit in a special / temporal dual mode PUF.

As explained above (see Fig. 9) the main hardware parts of the interrogation unit are the optical source, the input photonic encoder and the imaging unit (camera). Some years ago, these components were rather bulky and expensive, and the overall system was in most cases assembled on optical tables with strict vibration isolation and temperature stabilization requirements. Things have changed since and the current implementations appear to be very compact, low cost, and high performing with very good robustness and unclonability performance. Indeed, low cost and high emission quality VCSELS can be used in combination with miniature structure light units (e.g. MOEMS based), some micro-optics for the beam formation, sufficiently complex low cost disordered scattering media, and chip cameras with sufficient resolution and very small footprint (e.g. a surface of few mm^2). The first such implementation at a preproduction level was reported in [42], [43] and was tested successfully for a period of six months continuously in the framework of the EU R&D project SMILE [44].

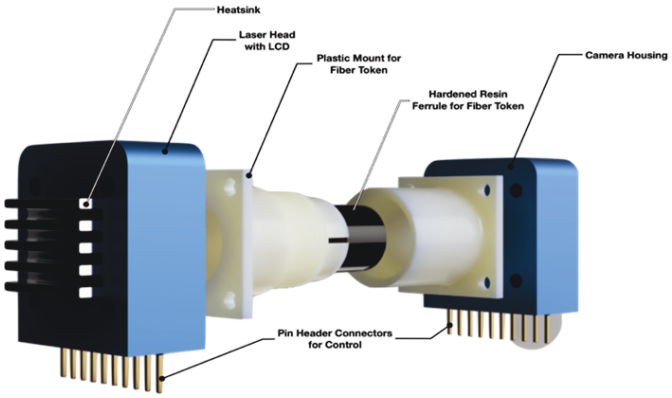

Fig. 9: Representation of the PUF main Unit as implemented in [42]. Courtesy of Eulambia Ltd.

The system is under further development with improved performance and much smaller footprint and power consumption towards a USB stick like implementation. Key role in the performance and the operation of the system plays the software which is responsible for transcription of the numerical challenges to the uncorreleted space structured light patterns that illuminate the token, AI assisted image processing techniques for the speckle stabilization / extraction, hashing, processing etc. All these, together with the conventional process of enrolment / authentication, helper data generation, etc. In conclusion, the speckle imaging based optical PUF with its inherent advantages of low cost, resistance to machine learning attacks, stable operation and potential for a very small footprint, is a very strong candidate appropriate for a broad range of cyber security applications.

References

[1] Y. Yilmaz, S. R. Gunn, and B. Halak, "Lightweight PUF-based authentication protocol for IoT devices," *2018 IEEE 3rd Int. Verif. Secur. Work. IVSW 2018*, pp. 38–43, 2018.

[2] M. M. Tehranipoor, U. Guin, and S. Bhunia, "Invasion of the hardware snatchers," *IEEE Spectr.*, vol. 54, no. 5, pp. 36–41, 2017.

[3] T. Cisco and A. Internet, "Cisco Annual Internet Report (2018–2023)," Tech. Rep. 3, 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1361372320300269

[4] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication Protocols for Internet of Things: A Comprehensive Survey," *Secur. Commun. Networks*, vol. 2017, 2017.

[5] P. Kocher, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom, "Spectre attacks: Exploiting speculative execution," in *2019 IEEE Symp. Secur. Priv.*, 2019. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8835233

[6] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, and M. Hamburg, "Meltdown," *https://arxiv.org/abs/1801.01207*, 2018.

[7] R. Pappu, "Physical One-Way Functions," Ph.D. dissertation, Massachusetts Institute of Technology, 2001.

[8] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Controlled physical random functions," in *Proc. - Annu. Comput. Secur. Appl. Conf. ACSAC*, vol. 2002-Janua, 2002, pp. 149–160.

[9] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security*. Springer, 2010, pp. 3–37.

[10] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[11] U. Rührmair and D. E. Holcomb, "Pufs at a glance," in *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2014, pp. 1–6.

[12] R. Falk and S. Fries, "New Directions in Applying Physical Unclonable Functions," in *Secur. 2015 Ninth Int. Conf. Emerg. Secur. Information, Syst. Technol. New*, 2015, pp. 31–36.

[13] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "Fpga intrinsic pufs and their use for ip protection," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2007, pp. 63–80.

[14] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-up sram state as an identifying fingerprint and source of true random numbers," *IEEE Transactions on Computers*, vol. 58, no. 9, pp. 1198–1210, 2008.

[15] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conference*. IEEE, 2007, pp. 9–14.

[16] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and U. Rührmair, "The bistable ring PUF: A new architecture for strong physical unclonable functions," in *2011 IEEE Int. Symp. Hardware-Oriented Secur. Trust. HOST 2011*, 2011, pp. 134–141.

[17] U. Rührmair, X. Xu, J. Sölter, A. Mahmoud, M. Majzoobi, F. Koushanfar, and W. Burleson, "Efficient power and timing side channels for physical unclonable functions," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2014, pp. 476–492.

[18] G. T. Becker, "The gap between promise and reality: On the insecurity of xor arbiter pufs," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2015, pp. 535–555.

[19] U. Ruhrmair, J. Solter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas, "PUF modeling attacks on simulated and silicon data," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 11, pp. 1876–1891, nov 2013. [Online]. Available: http://ieeexplore.ieee.org/document/6587277/

[20] J. Delvaux and I. Verbauwhede, "Side channel modeling attacks on 65nm arbiter PUFs exploiting CMOS device noise," in *Proc. 2013 IEEE Int. Symp. Hardware-Oriented Secur. Trust. HOST 2013*. IEEE, jun 2013, pp. 137–142. [Online]. Available: http://ieeexplore.ieee.org/document/6581579/

[21] U. Ruhrmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," *Proc. 17th ACM Conf. Comput. Commun. Secur. - CCS '10*, no. i, p. 237, 2010. [Online]. Available: http://dl.acm.org/citation.cfm?id=1866307.1866335

[22] B. T. Bosworth, I. A. Atakhodjaev, M. R. Kossey, B. C. Grubel, D. S. Vresilovic, J. R. Stroud, N. Macfarlane, J. Villalba, N. Dehak, A. B. Cooper, M. A. Foster, and A. C. Foster, "Unclonable photonic keys hardened against machine learning attacks," *APL Photonics*, vol. 5, no. 1, p. 010803, jan 2020. [Online]. Available: http://aip.scitation.org/doi/10.1063/1.5100178

[23] C. Zhou, K. K. Parhi, and C. H. Kim, "Secure and Reliable XOR Arbiter PUF Design: An Experimental Study based on 1 Trillion Challenge Response Pair Measurements," in *Proc. - Des. Autom. Conf.*, vol. Part 12828. Institute of Electrical and Electronics Engineers Inc., jun 2017.

[24] U. Rührmair, C. Hilgers, S. Urban, A. Weiershäuser, E. Dinter, B. Forster, and C. Jirauschek, "Optical PUFs Reloaded," *IACR Cryptol.*, 2013. [Online]. Available: https://eprint.iacr.org/2013/215.pdf http://eprint.iacr.org/2013/215.pdf

[25] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical One-Way Functions," *Science (80-.).*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[26] C. Sun, M. T. Wade, Y. Lee, J. S. Orcutt, L. Alloatti, M. S. Georgas, A. S. Waterman, J. M. Shainline, R. R. Avizienis, S. Lin, B. R. Moss, R. Kumar, F. Pavanello, A. H. Atabaki, H. M. Cook, A. J. Ou, J. C. Leu, Y. H. Chen, K. Asanović, R. J. Ram, M. A. Popović, and V. M. Stojanović, "Single-chip microprocessor that communicates directly using light," *Nature*, vol. 528, no. 7583, pp. 534–538, 2015. [Online]. Available: http://dx.doi.org/10.1038/nature16454

[27] M. T. Wade, F. Pavanello, J. Orcutt, R. Kumar, J. Shainline, V. Stojanovic, R. Ram, and M. Popovic, "Scaling zero-change photonics: An active photonics platform in a 32 nm microelectronics SOI CMOS process," in *CLEO Sci. Innov.* Optical Society of America, 2015, pp. SW4N—-1.

[28] B. C. Grubel, B. T. Bosworth, M. R. Kossey, H. Sun, A. B. Cooper, M. A. Foster, and A. C. Foster, "Silicon photonic physical unclonable function," *Opt. Express*, vol. 25, no. 11, p. 12710, 2017. [Online].

Available: https://www.osapublishing.org/abstract.cfm?URI=oe-25-11-12710

[29] F. Bin Tarik, A. Famili, Y. Lao, and J. D. Ryckman, "Robust optical physical unclonable function using disordered photonic integrated circuits," *Nanophotonics*, vol. 9, no. 9, pp. 2817–2828, sep 2020. [Online]. Available: https://doi.org/10.1515/nanoph-2020-0049

[30] H. Sun, M. Alemohammad, B. Bosworth, B. C. Grubel, A. B. Cooper, M. A. Foster, and A. Foster, "Photonic Physical Unclonable Functions using Silicon Nitride Spiral Cavities," *Conf. Lasers Electro-Optics*, p. STh1N.4, 2017. [Online]. Available: https://www.osapublishing.org/abstract.cfm?URI=CLEO_SI-2017-STh1N.4

[31] A. Rahim, E. Ryckeboer, A. Z. Subramanian, S. Clemmen, B. Kuyken, A. Dhakal, A. Raza, A. Hermans, M. Muneeb, S. Dhoore, Y. Li, U. Dave, P. Bienstman, N. Le Thomas, G. Roelkens, D. Van Thourhout, P. Helin, S. Severi, X. Rottenberg, and R. Baets, "Expanding the Silicon Photonics Portfolio with Silicon Nitride Photonic Integrated Circuits," *J. Light. Technol.*, vol. 35, no. 4, pp. 639–649, feb 2017. [Online]. Available: https://www.osapublishing.org/abstract.cfm?uri=jlt-35-4-639 https://www.osapublishing.org/jlt/abstract.cfm?uri=jlt-35-4-639

[32] G. Roelkens, U. Dave, A. Gassenq, N. Hattasan, C. Hu, B. Kuyken, F. Leo, A. Malik, M. Muneeb, E. Ryckeboer, D. Sanchez, S. Uvin, R. Wang, Z. Hens, R. Baets, Y. Shimura, F. Gencarelli, B. Vincent, R. Loo, J. Van Campenhout, L. Cerutti, J. B. Rodriguez, E. Tournie, X. Chen, M. Nedeljkovic, G. Mashanovich, L. Shen, N. Healy, A. C. Peacock, X. Liu, R. Osgood, and W. M. Green, "Silicon-based photonic integration beyond the telecommunication wavelength range," *IEEE J. Sel. Top. Quantum Electron.*, vol. 20, no. 4, 2014. [Online]. Available: http://ieeexplore.ieee.org.

[33] B. C. Grubel, B. T. Bosworth, M. R. Kossey, A. B. Cooper, M. A. Foster, and A. C. Foster, "Information-Dense Nonlinear Photonic Physical Unclonable Function," *https://arxiv.org/abs/1711.02222*, 2017.

[34] N. MacFarlane, J. R. Stroud, A. B. Cooper, M. A. Foster, and A. C. Foster, "Highly nonlinear amorphous silicon micro-cavity as a platform for secure authentication," in *FiO + Laser Science APS/DLS*. Optical Society of America, 2019, p. FTu1E.3.

[35] M. Akriotou, C. Mesaritakis, E. Grivas, C. Chaintoutis, A. Fragkos, and D. Syvridis, "Random number generation from a secure photonic physical unclonable hardware module," in *Commun. Comput. Inf. Sci.*, vol. 821. Springer Verlag, feb 2018, pp. 28–37. [Online]. Available: https://doi.org/10.1007/978-3-319-95189-8_3

[36] S. M. Popoff, G. Lerosey, R. Carminati, M. Fink, A. C. Boccara, and S. Gigan, "Measuring the transmission matrix in optics: An approach to the study and control of light propagation in disordered media," *Phys. Rev. Lett.*, vol. 104, no. 10, p. 100601, mar 2010. [Online]. Available: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.104.100601

[37] H. Yu, T. R. Hillman, W. Choi, J. O. Lee, M. S. Feld, R. R. Dasari, and Y. Park, "Measuring large optical transmission matrices of disordered media," *Phys. Rev. Lett.*, vol. 111, no. 15, p. 153902, oct 2013. [Online]. Available: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.111.153902

[38] Y. Li, Y. Xue, and L. Tian, "Deep speckle correlation: A deep learning approach towards scalable imaging through scattering media," *Optica*, vol. 5, no. 10, pp. 1181–1190, jun 2018. [Online]. Available: https://doi.org/10.1364/OPTICA.5.001181

[39] Q. Li, J. Zhao, Y. Zhang, X. Lai, Z. Chen, and J. Pu, "Imaging reconstruction through strongly scattering media by using convolutional neural networks," *Opt. Commun.*, vol. 477, p. 126341, dec 2020.

[40] C. Mesaritakis, M. Akriotou, A. Kapsalis, E. Grivas, C. Chaintoutis, T. Nikas, and D. Syvridis, "Physical Unclonable Function based on a Multi-Mode Optical Waveguide," *Sci. Rep.*, vol. 8, no. 1, p. 9653, dec 2018. [Online]. Available: www.nature.com/scientificreports/

[41] F. Chen, Q. Li, M. Li, F. Huang, H. Zhang, J. Kang, and P. Wang, "Unclonable fluorescence behaviors of perovskite quantum dots/chaotic metasurfaces hybrid nanostructures for versatile security primitive," *Chem. Eng. J.*, vol. 411, p. 128350, may 2021.

[42] M. Akriotou, A. Fragkos, and D. Syvridis, "Photonic Physical Unclonable Functions: From the Concept to Fully Functional Device Operating in the Field," in *Proc. SPIE 11274, Phys. Simul. Optoelectron. Devices XXVIII, 112740N (28 May 2020)*, vol. 11274. arXiv, feb 2020, p. 112740N. [Online]. Available: https://www.spiedigitallibrary.org/conference-proceedings-of-spie/11274/112740N/Photonic-physical-unclonable-functions–from-the-concept-to-fully/10.1117/12.2551272.full https://www.spiedigitallibrary.org/conference-proceedings-of-spie/11274/112740N/Photonic-physical-unclonable-functions–from-the-concept-to-fully/10.1117/12.2551272.short

[43] C. Chaintoutis, M. Akriotou, C. Mesaritakis, I. Komnios, D. Karamitros, A. Fragkos, and D. Syvridis, "Optical PUFs as physical root of trust for blockchain-driven applications," *IET Softw.*, vol. 13, no. 3, pp. 182–186, jun 2019. [Online]. Available: www.ietdl.org

[44] "SMart Mobility at the European Land boarders (SMILE)," pp. https://Smile–h2020.eu.