Exploiting randomly distributed pores in photonic structures for security applications to create hardware-based digital identity

David Martín-Sánchez[1,2], Piedad Brox[1]
[1]Instituto de Microelectrónica de Sevilla, IMSE-CNM (CSIC, Universidad de Sevilla), Spain
[2]Department of Medical Physics and Biomedical Engineering, University College London, UK

david.martin@imse-cnm.csic.es

Digital technology has transformed global economy and people's lifestyles in half a century by enhancing communications, trading, access to information, and processing capabilities. However, this technology also carried a series of serious threats to information and privacy [1]. For example, sensitive information can be exposed when transmitted through an unsecured communication channel, and industrial secrets can be stolen from an unprotected database. To address this issue, digital cryptography was developed.

A secure network infrastructure integrates a set of techniques to guarantee confidentiality, integrity, and availability of data and devices, which prevent or mitigate unauthorized access, data breaches, and malicious activities. In addition, these techniques are combined with data Privacy-Preserving Mechanisms (PPMs), which are crucial to protect users' privacy and their rights to have control over how their personal information is collected, processed, stored and shared. All these solutions rely on protocols and libraries that incorporate cryptographic algorithms [2].

Encryption and authentication procedures enable confidentiality and system verification to prove genuineness. Both are based on secret keys, i.e., strings of bits that are used to encode and decode information by means of cryptographic algorithms and as digital identifiers. These secret keys can be stored in non-volatile memories [3] (e.g., EEPROM), however this method increases the power consumption and footprint of devices as well as the risk of exposure [4]. As an alternative, secret keys are preferred to be generated on demand by using a cryptographic primitive known as a physical unclonable function (PUF).

A PUF is a device that generates a deterministic bit string (i.e., a response) when it is interrogated (i.e., challenged) by a particular physical probe, and can be generated as many responses as there are challenges. Different PUFs generate different responses to identical challenges (see Fig. 1), and each response is unique and very difficult to predict by any physical or computational mean. This behaviour can be exploited as a source for the reconstruction of cryptographic keys.

Practical implementations of PUFs need to ensure the uniqueness of the responses while being compatible with large-scale manufacturing at low cost. To achieve this, the random manufacturing variations of microelectronic circuits have been traditionally exploited to implement PUFs. For example, the small voltage threshold mismatches of transistors in a SRAM leads to a tendency towards either the '1' or '0' state of the unit cells during power up [5]. Hence, the map of bits in this initial phase can be used to identify each hardware device. Other PUF configurations make use of Ring Oscillators and exploit the slight variations of the resonant frequencies to extract a hardware fingerprint [6].

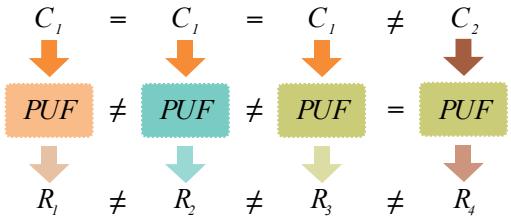

Figure 1. Behaviour of a set of Physical Unclonable Functions (PUFs) used to generate unique cryptographic keys on demand.

Unfortunately, electronic PUFs have been classified as weak against modelling attacks, as it is expected that emerging Machine Learning methods will be able to simulate the behaviour of these PUFs to predict their responses. This is due to the low number of available challenge-response pairs (CRPs) and the low entropy of the underlying physical mechanisms producing the variations [7].

As a more robust alternative, optical PUFs have been proposed [8]. Optical PUFs are considered strong against modelling attacks because they are based on complex mechanisms such as optical scattering or multimode interference [9,10]. In such cases, the PUF consists of disordered scatterers randomly distributed inside a physical medium or of interfaces with rough profiles. The probe is usually a light beam and the responses are typically measured as an optical intensity map at an output plane. The random optical interference pattern, known as speckle pattern (see Fig. 2), is sensible to variations of the probing light (such as wavelength, power, or angle of incidence) and variations of the physical medium (such as rotation, translation, or tilt). This behaviour is exploited to achieve a high number of CRPs producing numerous unique and random keys and digital identifiers.

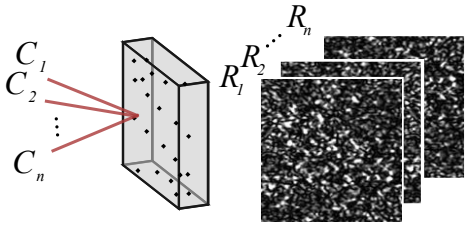

Figure 2. Optical PUF exploiting randomly distributed scatterers inside a medium, challenged by an optical probe of variable angle of incidence, resulting in different unique responses measured as speckle patterns at an output plane.

However, despite the advanced security advantages provided by optical PUFs, their research is still scarce and electronic PUFs are still preferred.

One of the reasons is the concern regarding the reliability of the responses over time due to aging of the materials and the precise alignment required between the PUF, the probing light and the readout scheme. Another reason for the low adoption of optical PUFs is their lack of miniaturisation and their incompatibility with large-scale CMOS manufacturing capabilities (especially in the case of Internet-of-Things and wearable devices [11]).

We propose the use of micro and nanophotonic structures based on porous materials [12] to develop novel optical PUFs. Many techniques have been researched to produce porous materials in a variety of complex arrangements, from uniformly distributed column-like pores to interconnected pores forming sponge-like structures. In addition, such porous structures can be designed with multidimensional periodicity to create photonic crystals [13], or as arrays with different properties [14]. The many degrees of freedom during the fabrication result in unique features, the size, orientation, and distribution of which are unfeasible to replicate, hence ensuring unclonability. Moreover, these highly complex devices remain in the micrometre scale, allowing the miniaturisation of the PUF and increasing their reliability due to a reduced exposure to environmental variations.

For this purpose, we have explored the use of porous polymer membranes containing randomly distributed micrometre-scale pores (220µm average pore size). Such membranes are commercially available (ICT S.L., Spain) and inexpensive, offering cylindrical pores randomly distributed over an area of 17cm^2 with 75% porosity. We used the pores as light scatterers, acting the whole membrane as a diffuser. As a light source, we employed a CW laser (632nm, 0.8mW, Thorlabs Inc., USA) and the resulting interference field was measured using a CMOS camera (Thorlabs Inc., USA). We exploited the large surface of the membrane to generate numerous cryptographic keys by interrogating different areas with the light beam whose spot size was 500µm.

We established that the responses were completely uncorrelated when the illuminated spots were separated 50µm. Hence, the proposed PUFs allowed over 10^7 unique CPRs. This was achieved using a simple lens-free optical setup. The extracted 256-bit cryptographic keys were obtained as the Gabor Transform [15] of the acquired speckle patterns. The Hamming Distance (HD) was calculated to determine the uniqueness of the response, which is a parameter that counts the number of bits that are different in two bit strings. Hence, equal bit strings result in HD=0 and two different and random bit strings result in HD=0.5. In our case, when the PUF was interrogated using the same challenge, we measured an HD=0.03. When different challenges were applied, we measured an HD=0.43. These results (shown in Fig. 3) demonstrate the suitability of the porous membranes to create strong hardware-based digital identifiers and cryptographic key generators.

We believe our work demonstrates the suitability of using porous structures to develop strong optical PUFs. In the future, other porous materials compatible with silicon-based microelectronics could be explored for device integration, such as porous silicon. In addition, other interrogation methods could be studied to enable on-chip generation of challenges, to increase reliability. Such PUFs would allow the generation of secure cryptographic keys which would help shortcoming the vulnerabilities of current electronic devices and avoid the disruption caused by cyberattacks.

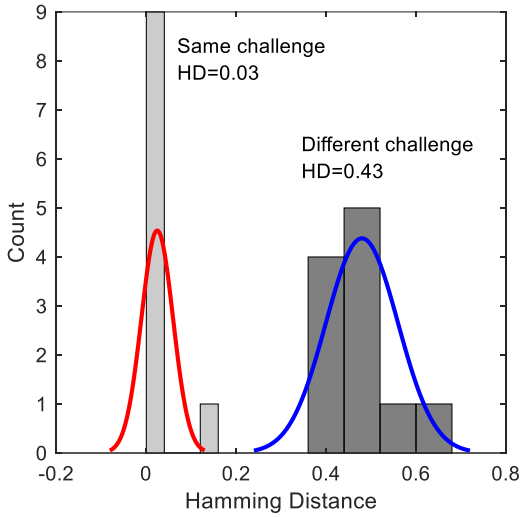

Figure 3. Uniqueness and reliability of the proposed optical PUF based on a porous membrane, characterised as the Hamming Distance between bit strings (number of bits that are different).

References

[1] B. van den Berg *et al.*, Oxford University Press (2022).
[2] C. Paar *et al.*, Springer (2010).
[3] V. Mikhalev, *et al.*, IACR Transactions on Symmetric Cryptology (2016).
[4] S. Ghosh, *et al.*, IEEE/ACM International Conference on Computer-Aided Design (2016).
[5] C. Herder, *et al.*, Proceedings of the IEEE 102(8) (2014).
[6] S. Lee, *et al.*, 9th International Conference on Information and Communication Technology Convergence (2018).
[7] B. T. Bosworth, *et al.*, APL Photonics 5(1), (2020).
[8] U. Rührmair, *et al.*, Cryptology ePrint Archive, Paper 2013/215, (2013).
[9] R. Pappu, *et al.*, Science, 297 (2002).
[10] C. Mesaritakis, *et al.*, Sci Rep 8(1), (2018).
[11] A. Al-Meer *et al.*, ACM Comput Surv 55(14 S), (2023).
[12] E. Monaico, *et al.*, Semicond Sci Technol 35(10), (2020).
[13] J. D. Joannopoulus, S *et al.*, Princeton University Press (2007).
[14] D. Martin-Sanchez, *et al.*, IEEE Sens J 20(15), 8497–8504 (2020).
[15] O. Nestares, *et al.*, J Electr Imaging 7(1), 166-173 (1998).