Universitat Autònoma de Barcelona

Dipòsit digital de documents de la UAB

This is the **accepted version** of the journal article:

Porti i Pujal, Marc; Redon, Miquel; Muñoz Gorriz, Jordi; [et al.]. «Oxide Breakdown Spot Spatial Patterns as Fingerprints for Optical Physical Unclonable Functions». IEEE electron device letters, Vol. 44, Issue 10 (October 2023), p. 1600-1603. DOI 10.1109/LED.2023.3301974

This version is available at https://ddd.uab.cat/record/283102

under the terms of the license

Oxide Breakdown Spot Spatial Patterns as Fingerprints for Optical Physical Unclonable Functions

Marc Porti, Miquel Redón, Jordi Muñoz, Montserrat Nafría, Enrique Miranda

Abstract— **Dielectric Breakdown (BD) of the gate oxide in a Metal-Insulator-Semiconductor (MIS) or Metal-Insulator-Metal (MIM) structure has been traditionally considered a major drawback since such event can seriously affect the electrical performance of the circuit containing the device. However, since BD is an inherently random process, when externally detectable by optical means, the phenomenon can be used to generate cryptographic keys for Physically Unclonable Functions (PUFs). This is the case discussed here. Images containing BD spot spatial distributions in MIM devices were binarized and their uniformity, uniqueness and reproducibility evaluated as fingerprints for security applications such as anti-counterfeiting purposes, secure identification and authentication of components. The obtained results are highly promising since it is demonstrated that the generated fingerprints meet all the mandatory requirements for PUFs, indicating that the proposed approach is potentially useful for this kind of applications.**

Index Terms— **Dielectric Breakdown, PUF, cryptography, MIM devices.**

I. INTRODUCTION

Dielectric Breakdown (BD) of the gate oxide in MIS or MIM structures has been traditionally considered a major reliability issue in micro- and nanoelectronic technologies. BD occurs when the gate dielectric loses its insulating property because of the action of electrical stress. BD is often detected as a sudden increase of the current flowing through the device which is ascribed to the formation of a defect-based percolation path spanning across the oxide layer. Although BD occurs in very small areas (namely, BD spots), that is, in the nanoscale range [1-6], if the process is not controlled, BD laterally propagates [7-9] and the damage becomes irreversible. Moreover, due to Joule heating effects, the localized shortcircuits can generate microexplosions [10, 11], leading to the appearance of marks or craters on the top electrode. In many cases, these marks can be detected by the naked eye or in more detail with an optical microscope [10, 12, 13]. This phenomenon is random in time and space so that these features (occurrence and location) are unpredictable. It is worth mentioning that randomness associated with BD was used in the past as a source of entropy in cryptography and security. True Random Number Generators (TRNGs) obtained from the first time-to-BD [14] and from current fluctuations registered after a soft-BD event [15] were also investigated for that purpose. Additionally, Physically Unclonable Functions (PUFs) [16-19] based on soft-BD currents [20] and on the breakdown spot location along the channel in MOS transistors [21] have been proposed.

It is worth emphasizing that all the above referred works rely on the measurement of some aspect of the electrical characteristics of the devices, so that in these cases additional circuitry is imperatively required for detection. Moreover, this kind of PUFs can be affected by extreme environments, such as high temperature and/or harmful radiation conditions since their conduction characteristics ultimately depend on the nanoscale properties of the materials [22]. On the contrary, BD spot spatial patterns are fully immune to such aggressive agents. Notice that optical PUFs have drawn the attention of developers because they can be used to generate irreproducible and unclonable fingerprints based on visual inspection and image processing without the need of adding a measuring unit to the product, which is highly beneficial for security applications in fields such as identification, authentication and anti-counterfeiting [23-27]. In this work, we demonstrate the feasibility of using BD spot spatial distributions generated in MIM devices by electrical stress and characterized by optical means as fingerprints for PUFs.

II. DETAILS OF THE PROPOSED OPTICAL PUF

The spatial distribution of BD spots has been studied in MIM devices ($Pt/HfO_2/Pt$) manufactured on a thick SiO_2 layer grown onto a Si substrate. The HfO_2 layer thickness is 30nm and was grown by Atomic Layer Deposition (ALD). Fig. 1a shows a typical cross section of the analyzed structures. The active area of the capacitors is 500 μm × 500 μm. In this work, 9 capacitors were stressed until BD by applying a constant voltage stress of -9V to the gate for 60 seconds. After the stress, optical images were obtained with an optical Microscope Nikon ECLIPSE LV150N, Bright Field, with long working distance objectives 10X, and were registered with a CMOS camera Moticam of 5 Megapixels resolution. Fig. 1b shows the image of one of the capacitors where the BD spots can be seen as black dots distributed across the top electrode of the capacitor. All images were obtained using identical illumination conditions and were used as the fingerprint of the corresponding PUF.

After image acquisition, the selection of the observation window within the capacitor area is critical in order to obtain reliable PUFs. For that purpose, an image like that shown in Fig. 1b was selected as reference. Then, in the active area of this image, a square area of 1320 pixels × 1320 pixels is defined by setting the location of its vertices. When a new image is registered, it is moved and rotated to match the reference one using the so-called phase correlation algorithm [28, 29]. Once this is done, all the images are aligned, at the same location and

This work was supported by Grant PID2019-103869RB-C32/AEI/10.13039/501100011033, 2017-SGR-954, PID2022-139586NB-C41 and Margarita Salas grant for the training of young doctors 2021-2023 funded by the EU–NextGenerationEU. M. Porti, M. Redón, J. Muñoz, M. Nafría and E. Miranda are with the Departament d'Enginyeria Electrònica, Universitat Autònoma de Barcelona, Barcelona 08193, Spain (e-mail: marc.porti@uab.es).We thank Dr. P. Hurley from Tyndall National Institute, Ireland, for sample provision and G. Abadal from UAB for making available the optical system.

with the same orientation. Afterwards, using the previously defined vertices, the analysis region (i.e. the area inside the frame in Fig. 1b) is determined for all the images. As a typical example, Fig. 2a shows optical images corresponding to two of the analyzed capacitors. In all cases, the analyzed images have a size of 1320 pixels × 1320 pixels, where each pixel has an area of ≈0.139 μm^2.

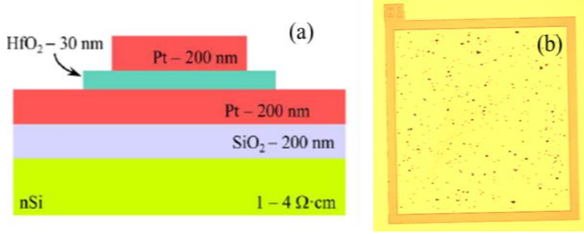

Fig. 1. (a) Schematics of the cross-section of the analyzed devices. (b) Top image of one of the investigated capacitors. The black dots are BD spots randomly generated during the electrical stress.

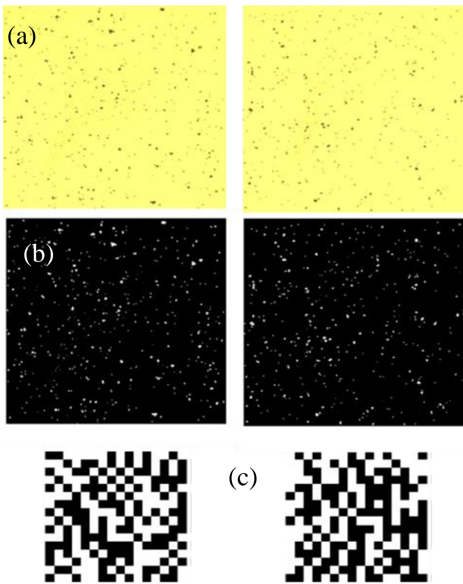

Fig. 2. (a) Optical images of two different capacitors (500 μm × 500 μm) and (b) their corresponding binarized maps. (c) Key maps obtained from the binarized optical images.

In order to generate the cryptographic keys once the observation windows are selected, the images are binarized. Such binarization is intended to show where the BD spots are located. The procedure is as follows: first, the image is split into three 2D matrices, one for each RGB primary color (red, green, and blue). Then, the values of these matrices are scaled in the range from 0 and 1, i.e., they are converted to a grayscale image for the specific color. Afterward, the matrices are binarized considering a selectable threshold value between 0 and 1. One threshold value for each color. Then, the three binary matrices are logically combined through an OR operator as some spots may only be detected in one of the separate images. Accordingly, Fig. 2b shows the binarized images corresponding to Fig. 2a. To improve the visualization aspect, the complementary image is considered here: "1" (white) represents the BD spots while "0" (black) represents regions where no spots are observed (see Fig. 2b). The methodology described above improves the detection of the spots found in the original optical image [10] as a lower sensitivity can be set for darker components (blue and green) and a higher one for the lighter component (red). For the investigated images, threshold values are 0.9, 0.9, and 0.2 for the red, green, and blue colors, respectively. The same values are used for all the PUFs investigated in this work. Note that the area corresponding to the BD spots (white regions) is smaller than the undamaged area (black regions). To eliminate the 0-bit bias and obtain uniform fingerprints, the classical von Newman (CVN) method was considered [30]. This method basically consists in, given a binary image, the bits are compared two by two. When both bits coincide, they are ruled out, otherwise only the first one is kept to generate the key. Using this debiasing method, a more balanced amount of 0's and 1's is reached [30]. After the debiasing process, the first 256 bits of each image were used to generate the cryptographic key for each PUF (map of 16 pixels x 16 pixels). Fig. 2c shows the key obtained for the images shown in Fig. 2b. In the authentication stage, the obtained fingerprint of a given capacitor is compared (from the intra-HD) and verified with the fingerprints of all generated PUFs, which should be pre-stored in a data center. For the sake of clarity, Fig. 3 summarizes de different stages necessary to generate the fingerprints from a stressed capacitor.

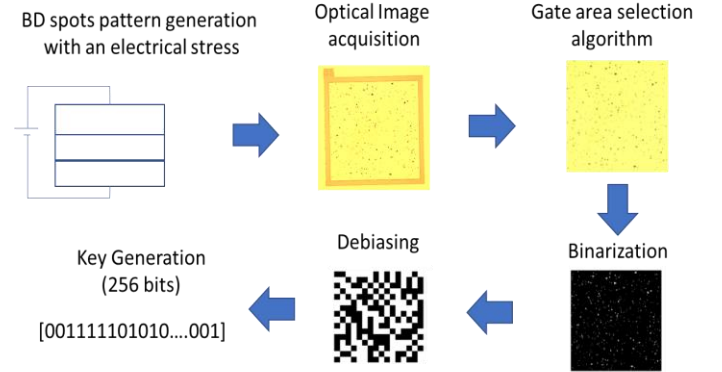

Fig. 3 Flowchart showing the generation of fingerprints from a capacitor.

III. Assessment of the PUFs Quality

In order to verify the quality of the generated PUFs, uniformity, uniqueness and reproducibility were analyzed. The bit uniformity, which is a measure of the random distribution of "0s" and "1s" is assessed first. The uniformity of a given PUF is evaluated by dividing the number of 0-bits by the total number of bits of the corresponding key, that is:

$$PUF\ Uniformity = \frac{1}{s}\sum_{i=1}^{s} K_i \ x\ 100\% \qquad (1)$$

where s is the key size and K_i the bit at location i in the PUF. In our case, the uniformity mean value and standard deviation (SD) for all the analyzed PUFs is 50.4% and 1.67%, respectively, with minimum and maximum values of 48.44% and 52.34%. Note that they are very close to 50%, the expected value for the ideal case.

To evaluate the degree of correlation between the binary keys of two different PUFs, the device uniqueness is assessed next. The device uniqueness is evaluated using the inter-device

Hamming Distance (HD). HD measures the number of bits that are different with respect to the total number of bits of the key when two different keys are compared. The inter-device HD between any two PUFs is defined as:

$$Device\ uniqueness = \frac{2}{q(q-1)} \sum_{i=1}^{q-1} \sum_{j=i+1}^{q} \frac{HD\ (K_i, K_j)}{s}\ x100\% \qquad (2)$$

where K_i and K_j are s-bit keys of the ith PUF device and the jth PUF device among q different PUFs, respectively. In our case, the 9 different PUFs available generate a total of 9x8/2=36 combinations. Fig. 4 illustrates the histogram corresponding to the normalized inter-device HD for all possible combinations. The average value is 49.72% with SD≈ 3.37%. These values are in close agreement with the 50% value expected for the ideal inter-device HD value.

The reproducibility of the same key when different images of the same capacitor are used was also evaluated. First, the stability of the BD spot distributions over time registered in the optical images was investigated. For this study, 2 images of the same capacitor (from the 9 studied PUFs) were taken with a time interval of 1.5 months. The images were obtained using the same microscope and camera, as well as identical illumination conditions. After binarization and debiasing, the obtained keys from both images (in each capacitor) were compared using the intra-HD distance, which provides the number of bits that underwent a change. The device reproducibility is then defined as:

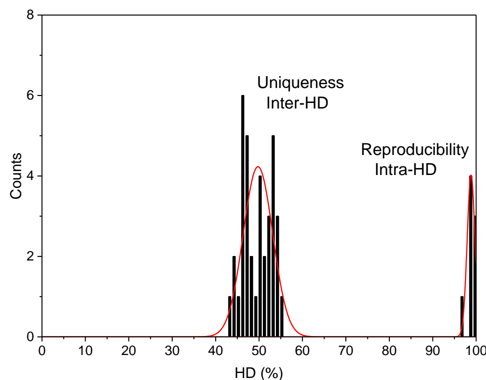

Fig. 4. Uniqueness and reproducibility obtained from 9 different PUFs. The average value is 49.72% (very close to the 50% ideal value), with a SD of 3.37% for the uniqueness and mean value 98.82% (very close to the 100% ideal value) with a SD of 0.89% for the device reproducibility.

$$Device\ reproducibility\ = (1 - \frac{HD\ (K_i, K_{i,t})}{s})\ x\ 100\% \qquad (3)$$

where K_i is the original s-bit reference and $K_{i,t}$ the s-bit key obtained from the same PUF after 1.5 months.

The result of this analysis is illustrated in Fig. 5. While Fig. 5a corresponds to an image of one of the analyzed capacitors, Fig. 5b shows the key obtained after applying the proposed methodology for the two images obtained from the same capacitor. In this case, the device reproducibility is about 98.44%, which is remarkably close to the ideal value of 100%. This analysis was conducted for the 9 capacitors investigated. The mean value and SD of the device reproducibility were found to be 98.82% and 0.89%, respectively, which indicates a high degree of coincidence. Fig. 4 shows the histogram corresponding to the reproducibility test. Importantly, notice that the uniqueness histogram does not overlap with the reproducibility one, which is an unambiguous evidence that the fingerprints obtained from the BD spot distributions are excellent candidates for the implementation of PUFs. Finally, the impact of other issues such as camera noise in the images or the *gate area selection algorithm* (due to unproper translation or rotation of the images) has also been evaluated. For this purpose, five images were taken of two of the analyzed capacitors and the intra-HD distance evaluated. The device reliability was then obtained using the same equation as for the device reproducibility (Eq. 3), obtaining a mean value and SD for the device reliability of 98.72% and 1.49%, indicating again a high degree of coincidence.

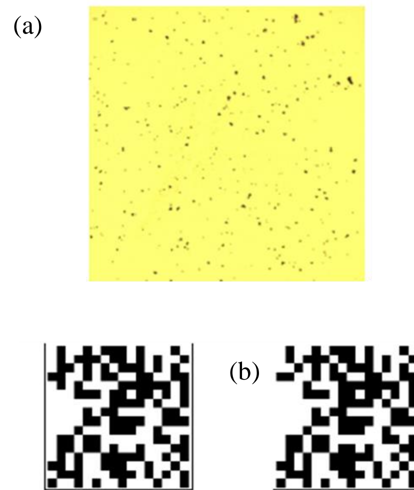

Fig. 5. Reproducibility of one of the analyzed PUFs (a) corresponds to the optical image while (b) shows the keys obtained from the images obtained with an interval of time of 1.5 months. In this case, the reproducibility is 98.82%

In summary, an innovative approach for the generation of PUFs based on BD spot spatial patterns generated in electrically stressed MIM structures was assessed. The stochastic nature of the oxide BD phenomenon together with the permanent and visible damage induced in the electrodes make the identification of fingerprints by optical means a feasible objective. Notice that the proposed methodology does not require extra circuitry as most of the previously proposed methods do. Only a test set-up is necessary to stress the devices until BD to generate the PUFs but this can be done beforehand. Although further work is necessary to evaluate the real implementation of PUFs based on this phenomenology, the obtained results indicate that the generated keys meet the essential requirements of uniformity, uniqueness, and reproducibility. Additionally, the proposed approach is fully compatible with conventional manufacturing technology of MIM devices.

REFERENCES

[1] J. Suné, I. Placencia, N. Barniol, E. Farrés, F. Martín, and X. Aymerich, “On the breakdown statistics of very thin SiO_2 films”, Thin Solid Films, vol. **185**, no. 2, pp. 347-362, 1990, doi: 10.1016/0040-6090(90)90098-X

[2] K. Shubhakar, K.L. Pey, N. Raghaban, S.S. Kushvaha, M. Bosman, Z. Wang and S.J. O’Shea, “Study of preferential localized degradation and breakdown of HfO2 /SiOx dielectric stacks at grain boundary sites of polycrystalline HfO2 dielectrics,” Microelectron. Eng., vol. 109, pp. 364–369, 2013. doi: 10.1016/j.mee.2013.03.021

[3] M. Lanza, G. Bersuker, M. Porti, E. Miranda, M. Nafría and X. Aymerich, “Resistive switching in hafnium dioxide layers: Local phenomenon at grain boundaries,” Appl. Phys. Lett., vol. 101, pp. 193502, 2012, doi: 10.1063/1.4765342

[4] U. Celano, Y. Y. Chen, D. J. Wouters, G. Groeseneken, M. Jurczak and W. Vandervorst, “Filament observation in metal-oxide resistive switching devices,” Appl. Phys. Lett., vol. 102, no. 12, pp. 121602, 2013, doi: 10.1063/1.4798525

[5] Y. L. Wu, J. J. Lin, B. T. Chen, C. Y. Huang, “Position-dependent nanoscale breakdown characteristics of thin silicon dioxide film subjected to mechanical strain,” IEEE Trans. Device Mater. Rel., vol. 12, no. 1, pp. 158–165, 2012, doi: 10.1109/TDMR.2011.2179804

[6] M. Porti, S. Meli, M. Nafría, X. Aymerich, “New insights on the post-BD conduction of MOS devices at the nanoscale”, IEEE Electron Device Letters, vol. 26, no. 2, pp. 109-111, doi: 10.1109/LED.2004.841190

[7] M. Porti, M. Nafria and X. Aymerich, “Current limited stresses of SiO2 gate oxides with conductive atomic force microscope”, IEEE Trans. Electron Devices, vol. 50, no. 4, pp. 933–940, 2003, doi: 10.1109/TED.2003.812082.

[8] S. Claramunt, Q. Wu, M. Maestro, M. Porti, M.B. Gonzalez, J. Martín-Martinez, F. Campabadal, M. Nafría, “Non-homogeneous conduction of conductive filaments in Ni/HfO2/Si resistive switching structures observed with CAFM”, Microelectron. Eng., vol. 147, pp. 335-338, 2015, doi: 10.1016/j.mee.2015.04.112

[9] M. Porti**,** M. Nafría, M. C. Blüm, X. Aymerich, S. Sadewasser, “Atomic Force Microscope topographical artifacts after the dielectric breakdown of ultrathin SiO_2 films”, Surface Science, Vol. 532-535, pp. 727-731, 2003. doi: 10.1016/S0039-6028(03)00150-X

[10] J. Muñoz-Gorriz, D. Blachier, G. Reimbold, F. Campabadal, J. Suñé, S. Monaghan, K. Cherkaoui, P. K. Hurley, E. Miranda, “Assessing the correlation between location and size of catastrophic breakdown events in high-K MIM capacitors”, IEEE Trans. Device Mater. Rel., vol. 19, no. 2, pp. 452-460, 2019, doi: 10.1109/TDMR.2019.2917138.

[11] G. Martín, M. B. González, F. Campabadal, F. Peiró, A. Cornet and S. Estradé, “Transmission electron microscopy assessment of conductive-filament formation in Ni-HfO2-Si resistive-switching operational devices”, Appl. Phys. Express, vol. 11, no. 1, p. 014101, 2018, doi: 10.7567/APEX.11.014101

[12] J. Muñoz-Gorriz, S. Monaghan, K. Cherkaoui, J. Suñé, P. K. Hurley, E. Miranda, “Exploratory study and application of the angular wavelet analysis for assessing the spatial distribution of breakdown spots in Pt/HfO2/Pt structures”, J. App. Phys., vol. 122, no. 21, p. 215304, 2017, doi: 10.1063/1.5000004

[13] J. Muñoz-Gorriz, S. Monaghan, K. Cherkaoui, J. Suñé, P. K. Hurley, E. Miranda, “Characterization of the failure site distribution in MIM devices using zoomed wavelet analysis”, J. Electron. Mater., vol. 47, no. 9, pp. 5033-5038, 2018, doi: 10.1007/s11664-018-6298-2

[14] N. Liu, N. Pinckney, S. Hanson, D. Sylvester, D. Blaauw, “A true random number generator using time-dependent dielectric breakdown”, IEEE 2011 Symposium on VLSI Circuits - Digest of Technical Papers, 21-1, June 2011.

[15] S. Yasuda, H. Satake, T. Tanamoto, R. Ohba, K. Uchida, S. Fujita, “Physical random number generator based on MOS structure after soft breakdown”, IEEE J. of Solid-state circuits, vol. 39, no. 8, pp. 1375-1377, 2004, doi: 10.1109/JSSC.2004.831480

[16] E. R. Hsieh *et al.*, "Positive-Bias-Temperature-Instability Induced Random-Trap-Fluctuation Enhanced Physical Unclonable Functions on 14-nm nFinFETs," in *IEEE Electron Device Letters*, vol. 43, no. 9, pp. 1396-1399, Sept. 2022, doi: 10.1109/LED.2022.3188492.

[17] D. Arumí, Á. Gómez-Pau, S. Manich, R. Rodríguez-Montañés, M. B. González and F. Campabadal, "Unpredictable Bits Generation Based on RRAM Parallel Configuration," IEEE Electron Device Letters, vol. 40, no. 2, pp. 341-344, Feb. 2019, doi: 10.1109/LED.2018.2886396.

[18] J. -W. Jung et al., "Concealable Oscillation-Based Physical Unclonable Function With a Single-Transistor Latch," IEEE Electron Device Letters, vol. 43, no. 8, pp. 1359-1362, Aug. 2022, doi: 10.1109/LED.2022.3182754.

[19] Y. Pang *et al.*, "Optimization of RRAM-Based Physical Unclonable Function With a Novel Differential Read-Out Method," IEEE Electron Device Letters, vol. 38, no. 2, pp. 168-171, Feb. 2017, doi: 10.1109/LED.2016.2647230.

[20] K. H. Chuang, E. Bury, R. Degraeve, B. Kaczer, D. Linten, I. Verbauwhede, “A physically unclonable function using soft oxide breakdown featuring 0% native BER and 51.8fJ/bit in 40-nm CMOS”, IEEE J. of Solid-state circuits, vol. 54, no. 10, pp. 2756-2776, 2019, doi: 10.1109/JSSC.2019.2920714

[21] K. H. Chuang, E. Bury, R. Degraeve, B. Kaczer, T. Kallstenius, G. Groseneken, D. Linten, I. Verbauwhede, “A Multi-bit/cell PUF using analog breakdown positions in CMOS”, 2018 IEEE International Reliability Physics Symposium (IRPS), P-CR.2-1, 2018, doi: 10.1109/IRPS.2018.8353655

[22] A. Cathignol *et al.*, "Quantitative Evaluation of Statistical Variability Sources in a 45-nm Technological Node LP N-MOSFET", IEEE Electron Device Letters, vol. 29, no. 6, pp. 609-611, June 2008, doi: 10.1109/LED.2008.922978.

[23] J.W. Leem, M.S. Kim, S.H. Choi, S.R. Kim, S.W. Kim, Y. M. Song, R. J. Young, Y. L. Kim, “Edible unclonable functions”, *Nat Commun vol.* **11**, 328, 2020, doi: 10.1038/s41467-019-14066-5

[24] Ahmet Turan Erozan, Michael Hefenbrock, Michael Beigl, Jasmin Aghassi-Hagmann, and Mehdi B. Tahoori, “Image PUF: A Physical Unclonable Function for Printed Electronics based on Optical Variation of Printed Inks”, IEEE Trans. On Information Forensics and security, 2019/1419, pp. 1-9.

[25] B. Wigger, T. Meissner, A. Förste, V. Jetter, A. Zimmermann, “Using unique surface patterns of injection moulded plastic components as an image based Physical Unclonable Function for secure component identification”, Scientific Reports, vol. 8, 4738, 2018, doi: 10.1038/s41598-018-22876-8

[26] B.H. Wu, C. Zhang, N. Zheng, L.W. Wu, Z.K. Xu, L.S. Wan, “Grain boundaries of self- assembled porous polymer films for unclonable anti-counterfeiting”, ACS Appl. Polym. Mater, vol. 1, no. 1, pp. 47-53, 2018, doi: 10.1021/acsapm.8b00031

[27] N. Torun, I. Torun, M. Sakir, M. Kalay, M. Serdar, “Physically unclonable surfaces via dewetting of polymer thin films”, ACS Appl. Mater. Interfaces, vol. 13, no. 9, pp. 11247-11259, 2021, doi: 10.1021/acsami.0c16846

[28] C. D. Kuglin, D. C. Hines, “The Phase Correlation Image Alignment Method”, Proceedings of the IEEE International Conference on Cybernetics and Society; San Francisco, USA. 23–25 September 1975; pp. 163–165

[29] B.S. Reddy, B. N. Chatterji, “An FFT-based technique for translation, rotation, and scale-invariant image registration”, IEEE Transactions on Image Processing, Vol. 5, no. 8, pp. 1266-1271, 1996, doi: 10.1109/83.506761

[30] R. Maes, V. van der Leest, E. van der Sluis and F. Willems, “Secure key generation from biased PUFs: Extended version”, J. Cryptographic Eng., vol. 6, pp. 121-137, 2016, doi: 10.1007/s13389-016-0125-6.