IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 22 December 2024, accepted 13 February 2025, date of publication 17 February 2025, date of current version 24 February 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3543000

RESEARCH ARTICLE

Reliability Assessment of Optical Physical Unclonable Functions Based on the Spatial Distribution of Catastrophic Failure Sites in MIM Structures

MARC PORTI, (Member, IEEE), ALVARO SOLIS, ALEX CALATAYUD, MONTSERRAT NAFRÍA, (Senior Member, IEEE), AND ENRIQUE MIRANDA, (Senior Member, IEEE)

Departament d'Enginyeria Electrònica, Universitat Autònoma de Barcelona, 08193 Bellaterra, Spain

Corresponding author: Marc Porti (marc.porti@uab.es)

This work was supported in part by the Ministerio de Ciencia e Innovación (MCIN)/Agencia Estatal de Investigación (AEI)/10.13039/501100011033/FEDER, European Union (UE), under Grant PID2022-139586NB-C41 and Grant PID2022-136949OB-C22; and in part by Grant 2021 SGR 00199.

ABSTRACT Catastrophic failure sites, also referred to as breakdown spots, in Metal-Insulator-Semiconductor (MIS) and Metal-Insulator-Metal (MIM) structures are the consequence of the formation of conducting paths across the thin oxide film that separates the contact electrodes. When the energy released by the sudden occurrence of this kind of shorts is high enough, the events are clearly detected in the top area of the structure as a random spatial point pattern. As it was demonstrated in previous works, the distribution of failure sites obtained this way can be used to generate optically detectable cryptographic keys in the context of Physically Unclonable Functions (PUFs). In this paper, we pay special attention to the reliability of the associated fingerprints. Reliability is evaluated in terms of a number of features of the binarized images such as the rotation and translation of the observation window, resolution, illumination, noise conditions, and particularities of the used optical system. The obtained results demonstrate that the generated fingerprints meet the essential requirements of reliability, reaching values between ∼90 and 99% in all the considered scenarios. By means of a simulated experiment, which closely resembles the practical application of the proposed method, we are able to assess how good the identification of the registered images is and therefore the feasibility of the considered approach. To complete the picture, the investigated PUFs are shown to be resilient to temperature and electrical stress attacks which makes them highly suitable for security applications.

INDEX TERMS Breakdown, cryptography, dielectric breakdown, MIM, MIS.

I. INTRODUCTION

The most important failure event occurring in MIS and MIM structures is that associated with the formation of a breakdown (BD) conducting path in between the top and bottom electrodes. This happens when a critical density of defects is locally reached because of the action of a severe electrical stress causing a short with irreversible consequences. While the occurrence of a BD event is often merely detected as a sudden increment of the current flowing through the device [1], [2], [3], [4], [5], [6], [7], [8], [9], catastrophic BD events are those associated with the generation of crater-like structures in the top surface of the device. The energy released during these events is so high that causes the local melting and evaporation of the top metal electrode [10], [11]. At the end, these microexplosions are clearly visible by the naked eye or through a microscope as a spatial point pattern [10], [12], [13]. Because of the random nature in time and space of this

The associate editor coordinating the review of this manuscript and approving it for publication was Chuan Li.

phenomenon, the distribution of BD sites in these devices has been suggested as an entropy source for cryptographic keys. In this regard, we can mention the proposal of True Random Number Generators (TRNGs) obtained from the first time-to-BD distributions [14] and from the current fluctuations occurring after a soft-BD event in MIS devices [15] as well as Physically Unclonable Functions (PUF) [16], [17], [18], [19], [20] based on the current magnitude [21], [22] and BD spot location along the channel of a MOS transistor [23]. It is worth emphasizing that all these methods rely on a particular set of electrical measurements so that, in general, additional circuitry is necessary to get and process the required information. Moreover, some CMOS-based PUFs are sensitive to hard environments, such as harmful radiation conditions and high temperatures [24], [25]. This happens because their electrical characteristics ultimately depend on the microscopic properties of the materials [26]. Devices can also be affected by additional electrical stresses, either due to unexpected operational conditions or to intentional external attacks [27]. Therefore, having arrived at this point, it becomes essential to examine the impact of environmental and use conditions, such as temperature and electrical stresses, on the PUFs functionality in order to both evaluate their impact on their electrical characteristics and identify potential threats related to these factors.

In recent years, optical PUFs [28], [29], [30], [31], [32] have drawn the attention of developers because they can be used to generate cryptographic keys based on visual inspection and image processing without the need of adding circuitry to the product. These particularities are not only extremely beneficial for security applications such as authentication, identification and anti-counterfeiting [33], [34] but also in terms of associated cost. In [35], we demonstrated, in the framework of a preliminary study, that images of oxide failure site spatial patterns met essential requirements such as homogeneity, uniqueness and time stability. However, in that work, the reliability aspect of the investigated structures was not considered, and this is also a crucial requirement for the PUF practical implementation. In this work, a detailed study about the reliability of the proposed PUFs is performed. To this end, we have evaluated different aspects such as the algorithm used to select the gate area of the device (which is crucial to compare the images obtained by the final user with those stored in the database), the effect of the image resolution, their illumination conditions, the noise introduced by the camera setup, and the role of the implemented optical system. Finally, intentional attacks were also simulated by applying severe electrical stress and large temperature excursions to the investigated devices.

II. STRUCTURE OF THE OPTICAL PUFS

In this work, we used MIM devices with an active area of 500 μm $\times$ 500 μm and with Pt as electrodes and HfO_2 (30nm thick, grown by Atomic Layer Deposition, ALD) as gate oxide. The MIM capacitors were manufactured on a thick SiO_2 layer grown onto a Si substrate. The cross section of the analysed structures is shown in Fig. 1. For the PUF's proof of concept demonstration, 9 capacitors (selected so as to show a variety of patterns) were evaluated as PUFs, which from here on will be called PUF_i, $1 \leq i \leq 9$ being the number of the investigated device.

The different steps followed to generate the fingerprints are illustrated in Fig. 2. First, a constant voltage stress (applied to the top electrode of the capacitor for 60 seconds) was used to induce BD (Fig. 2a). In this work, a voltage of -12V (higher than that considered in [35], where a voltage of -9V was used) was applied, in order to induce a higher number of BD spots. In this way, the damaged region of the devices increases with respect to their total area. After the stress, optical images (Fig. 2b) were obtained with the *optical system 1*. The system consists of an optical Microscope Nikon ECLIPSE LV150N with Bright or Dark Field and long working distance objectives 10X and with and integrated CMOS camera Moticam and 5 megapixels. Fig. 3 shows the optical images in Bright (left) and Dark (right) field obtained from the 9 stressed capacitors. Black (white) regions in the Bright (Dark) field images, respectively, correspond to the BD spots that were generated during the electrical stress. The images shown in Fig. 3 are considered as the references for each device. Note that, for identical stress conditions, different densities of BD spots can be obtained. While in some images the density is very high, as in the case of PUF_5, in others, such as PUF_4 or PUF_7, the density is quite low. We will demonstrate in Section IV that this particular issue does not affect the reliability of the PUF.

Once the image is obtained, choosing the appropriate observation window becomes a necessary step to achieve reliable PUFs. To this end, the image shown in Fig. 2c was selected as the reference [35]. A square area with 1336 pixels $\times$ 1336 pixels is chosen therein by setting the location of its vertices (Fig. 2c). New images are moved and rotated so as to match the reference one using the so-called phase correlation algorithm [36], [37]. The objective is to align all the involved images for making a reliable comparison. Taking into account the selected vertices, the analysis region (i.e. the area inside the frame in Fig. 2c) is finally determined for all the available images [35].

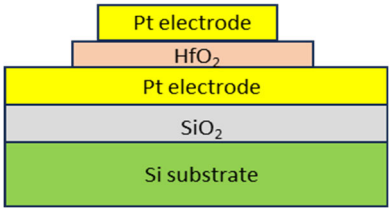

FIGURE 1. Cross-section of the analyzed MIM structures.

Once the observation window is selected, the binary word for a given PUF is generated by binarizing the corresponding image. This process is carried out with the aim of determining the spatial location of the BD spots. More in detail, the

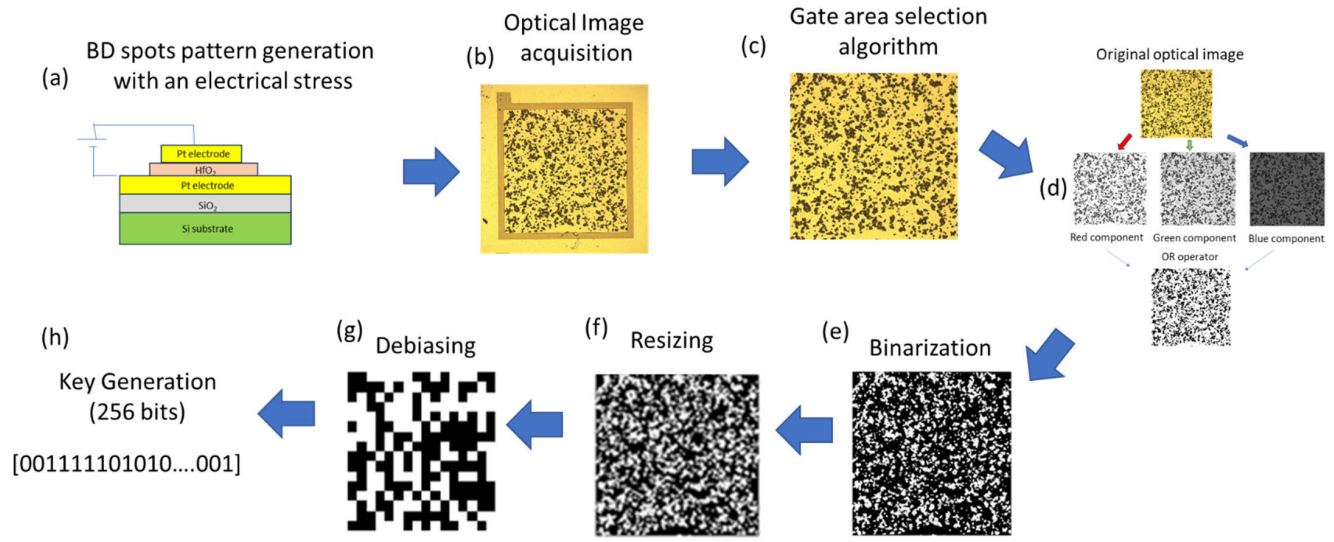

FIGURE 2. Flowchart showing the generation of fingerprints from a capacitor.

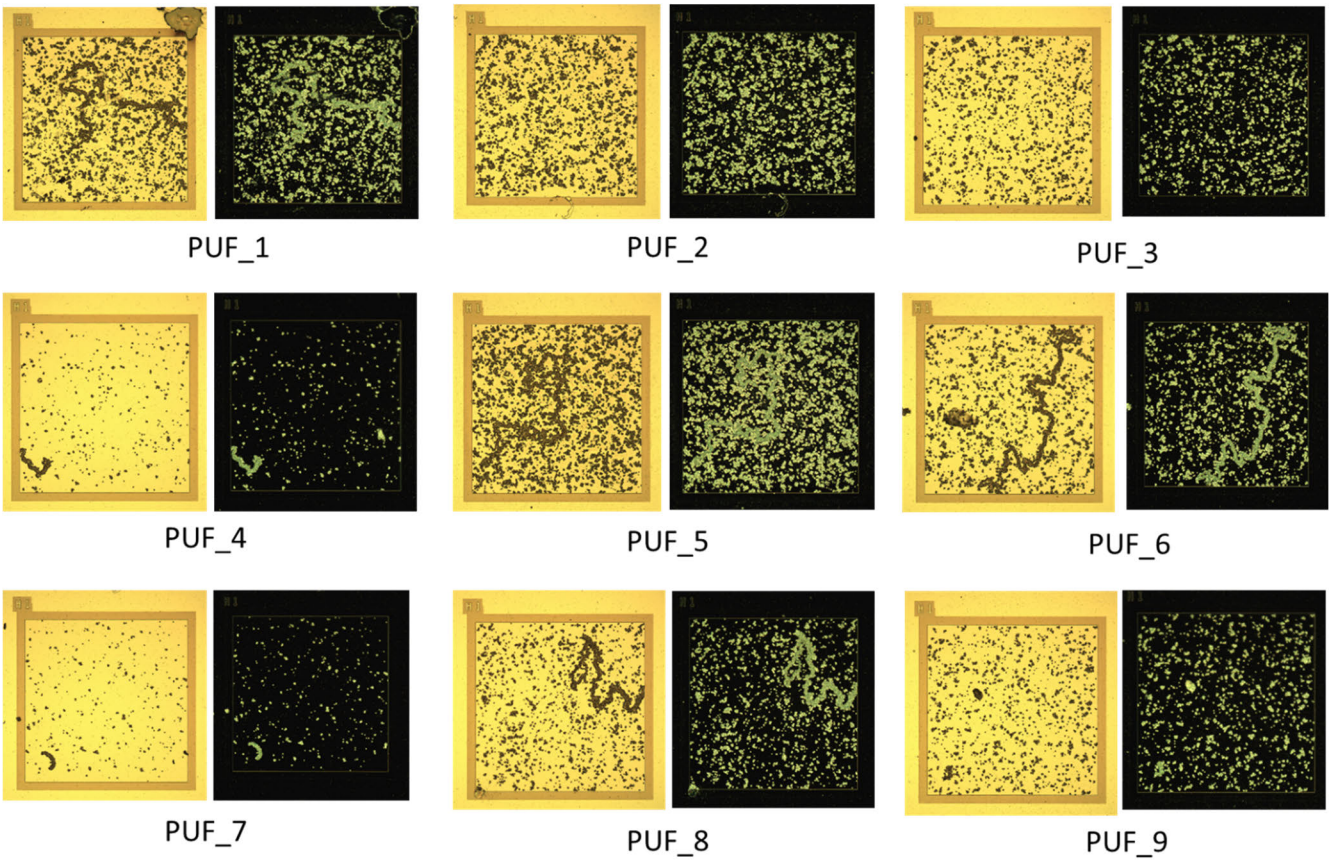

FIGURE 3. Bright (left) and Dark (right) Field optical images of the 9 investigated capacitors. The black (bright) regions correspond to the randomly generated BD spots during the electrical stress in the Bright (Dark) field images. These are the reference images that will be considered for the evaluation of the reliability.

procedure is as follows [35]: first, the image is filtered into three 2D matrices, one for each RGB primary color (red, green and blue). Then, the obtained values are proportionally scaled in the range [0,1]. Now, the images are grayscale for each specific color (Fig. 2d). Subsequently, the matrices are binarized assuming a threshold value for each color

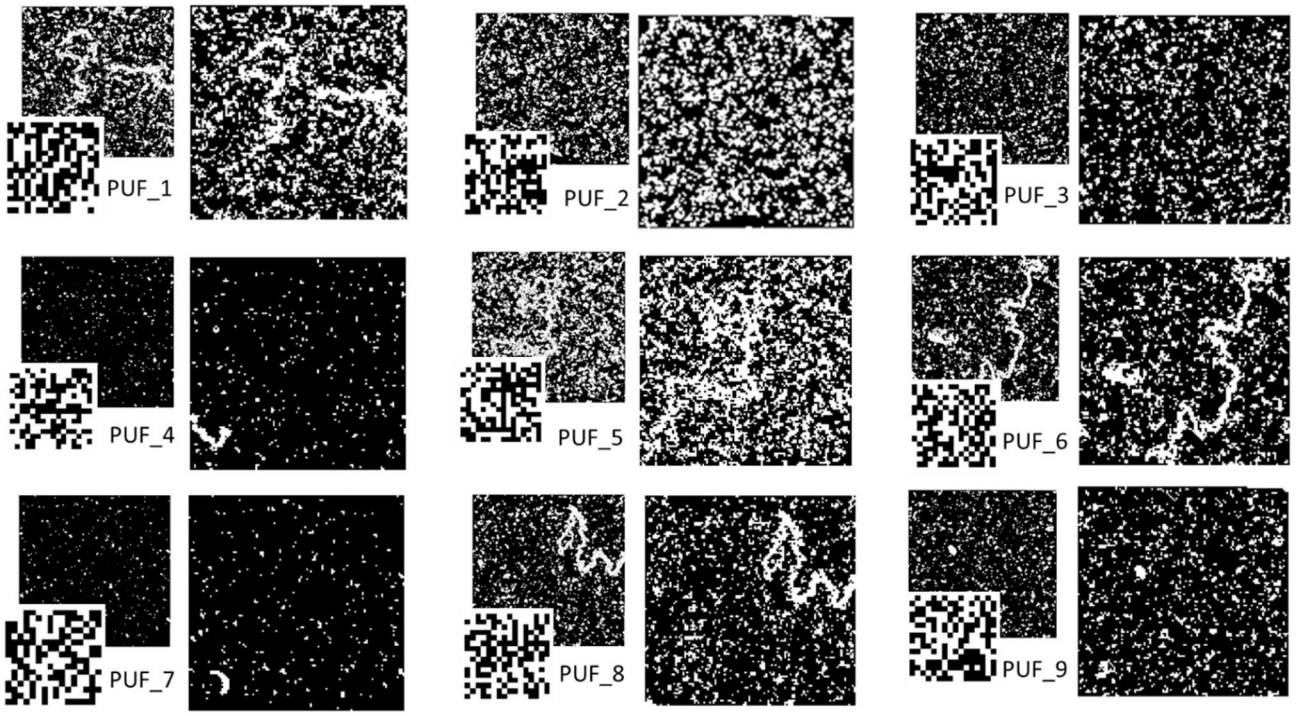

FIGURE 4. For each of the 9 analyzed PUFs, the figure shows (on the right) the maps (1336 pixels x 1336 pixels) after the binarization of the optical images in Fig. 3. Bright Field images are only shown. Binary maps obtained after Resizing the 1336 pixels x 1336 pixels images to 112 pixels x 112 pixels are shown on the left (top). 16 × 16 binary maps after the application of the CVN method are shown on the left (bottom).

component. Then, the three binary matrices are logically merged using an OR operator as some spots might only have been detected in one of the split images exclusively [35]. For illustrative purposes, Fig. 2e shows the binarized image corresponding to Fig. 2c. Note that from Fig. 2d to Fig. 2e the image has been inverted for visual purposes only. In our case, ''1'' (white) corresponds to the location of a BD spot while ''0'' (black) corresponds to an undamaged area (see Fig. 2e). The proposed methodology largely improves the identification of the spots detected in the optical image [10] as a lower sensitivity can be set for darker color components (blue and green) and a higher one for the lighter color component (red). Fig. 4 (right) shows the binarized maps of the images shown in Fig. 3 Bright Field. For the binarization of the images shown in Fig. 3 Bright Field, which are the references to which all the other images obtained in Bright Field are compared, we used the threshold values of 0.55, 0.5, and 0.23 for the red, green, and blue colors, respectively. Instead, for the images obtained in Dark Field (Fig. 3 right), threshold values of 0.24, 0.22 and 0.13 for the red, green and blue colors were used. After binarization, a preprocessing step was performed in order to reduce the size of the images (Fig. 2f). A resizing method is sometimes applied in order to generate binary keys from the optical images [30]. In this case, the size of the binarized optical image was reduced from 1336 × 1336 pixels to 112 × 112 pixels. The images of the PUFs after this process are illustrated in Fig. 4 (left).

It is worth mentioning that, though higher voltages than those used in [35] were considered in this work to generate the BD spots, the damaged area after binarization (Fig. 4, white regions) is still smaller than the undamaged area (black regions). To correct this asymmetry and therefore to obtain more uniform fingerprints, the classical von Newman (CVN) method was applied [38]. This method basically consists in, given a binary image, comparing adjacent bits two by two. When both bits coincide they are eliminated, 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 finally reached [38]. 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. 2g and Fig. 4 bottom). Fig. 2h shows a section of the key obtained for the image shown in Fig. 2b. Importantly, during the authentication stage, i.e. when the potential user takes an image of one capacitor, the described process needs to be performed in order to obtain the associated fingerprint, which is then compared (from the intra-Hamming Distance, intra-HD) with all the prestored fingerprints in the database. An emulation of the authentication stage is thoroughly described in Section V.

III. UNIFORMITY AND UNIQUENESS OF THE PUFS

Though the uniformity and uniqueness of the PUFs were already addressed in [35], for the sake of completeness, these features are briefly described for all the investigated PUFs. Recall that the uniformity of a PUF evaluates how comparable

the fraction of "0s" and "1s" is in the investigated devices. For ideal random PUF fingerprints, the uniformity is 50%. The uniformity of a PUF can be evaluated by dividing the number of 0-bits by the total number of bits of the key, and is defined by Equation (1):

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

where s is the key size and K_i the bit value at location i in the PUF. In our case, the uniformity of each PUF and their mean value and standard deviation (SD) were estimated for three cases: (i) for the binarized images obtained after resizing (Fig. 4, left), (ii) in the resized images after the application of the CVN and (iii) when considering only the first 256 bits of each image after the application of the CVN (Fig. 4, bottom), which correspond to the cryptographic key of each PUF (map of 16 pixels x 16 pixels). The mean and SD of the uniformities of the available PUFs are reported in Table 1. Note that, before the application of the CVN method, the uniformity is quite poor because the number of bits corresponding to the undamaged areas are in general higher than those in the areas corresponding to the catastrophic failure sites (specially, for instance, for PUF_4 and PUF_7, see Fig. 4). Therefore, the average uniformity is far away from the ideal case. However, after CVN and when the first 256 pixels are considered after its application, the uniformity of all the PUFs becomes better (it does not matter whether the images had many or few BD spots) and their averages are close to the ideal mean value, that is 50%, with a very low SD. In particular, for the 16 pixels x 16 pixels maps, a mean value of 50.95% is found. These results point out that the application of the CVN method indeed yields uniform PUFs.

The uniqueness represents the capacity of a PUF to generate a distinctive fingerprint for each particular PUF. In a wide sense, this estimator provides information about the degree of correlation between the binary keys of two different PUFs and ideally should be 50%. In this work, the device uniqueness is evaluated using the inter-device Hamming Distance (HD), which determines the number of bits that are different with respect to the total number of bits of the key when two different PUFs are compared. The inter-device HD is defined by equation (2):

$$Device\ uniqueness = \frac{2}{q(q-1)}\sum_{i=1}^{q-1}\sum_{j=i+1}^{q}\frac{HD(K_i, K_j)}{s}\ x\ 100\% \qquad (2)$$

where K_i and K_j are s-bit keys of the i^{th} PUF device and the j^{th} PUF device among q different PUFs, respectively. In our case, the 9 different PUFs lead to $9 \times 8/2 = 36$ combinations. We only evaluated the uniqueness for the case corresponding to the first 256 bits obtained after the application of the CVN (i.e., case iii). The mean and SD values for the investigated devices is reported in Table 1. Note that the average value is 50.46% with SD = 2.93%, which is very close to the ideal inter-device HD value (50%).

IV. RELIABILITY OF THE PUFS

In this Section, the reliability of the PUFs, i.e. the reproducibility of the generated fingerprints, is investigated in detail. To evaluate the reliability of a PUF different images of the same capacitor are required and the intra-HD distance is considered. This means that after binarization and debiasing, the obtained keys from the different images (in each capacitor) are compared in order to detect the number of bits that underwent a change. The reliability of a PUF is defined by equation (3):

$$Reliability = (1 - \frac{HD\left(K_i, K_{i,t}\right)}{s})x100\% \qquad (3)$$

where K_i is the original s-bit reference and $K_{i,t}$ the s-bit key obtained from another image of the same PUF. Ideally, reliability must be 100%. Since, for the evaluation of (3), two different images need to be compared, from now on, unless stated otherwise, the CVN is applied to the reference one exclusively. For the comparison with the second image, only the bits that were not ruled out in the first image are considered for the evaluation of the intra-HD.

Following the above procedure, the reliability of the proposed PUFs was evaluated taking into account different aspects that can affect the final outcome. For example, the **algorithm used to select the gate area of the device,** which is crucial for the comparison of images obtained by the final user with those stored in the database (Section A) was evaluated. The variety of **conditions** under which the final user takes the images (compared to the reference ones), as resolution and illumination are analyzed in Section B. In Section C, possible external **attacks** are simulated by applying severe electrical stress and high temperatures to the devices, which may induce additional BD spots. Finally, in Section D, the consequences of using an alternative **optical system** to that employed to get the reference images is assessed. In the following, images of PUF_2 are considered as illustrative examples.

A. GATE AREA SELECTION ALGORITHM: CAMERA NOISE, TRANSLATION AND ROTATION

When different images are compared for the evaluation of the PUF reliability, it is likely the occurrence of unexpected translations or rotations. To solve this problem, it is of utmost importance considering an algorithm able to select the same observation window in both images. In this section, the used *gate area selection algorithm* is evaluated by comparing images obtained from the 9 translated and rotated capacitors under investigation. In addition, the noise introduced by the optical system cannot be overlooked. In this regard, to evaluate the noise impact, for each capacitor, two different images obtained without moving the sample (that is, avoiding translations and rotations) were compared. In the analysis performed in this Section, all images were obtained in Bright Field using the same microscope and camera (*optical system 1*), as well as identical illumination conditions. As an example, for PUF_2, in order to evaluate the impact of the camera noise, translation

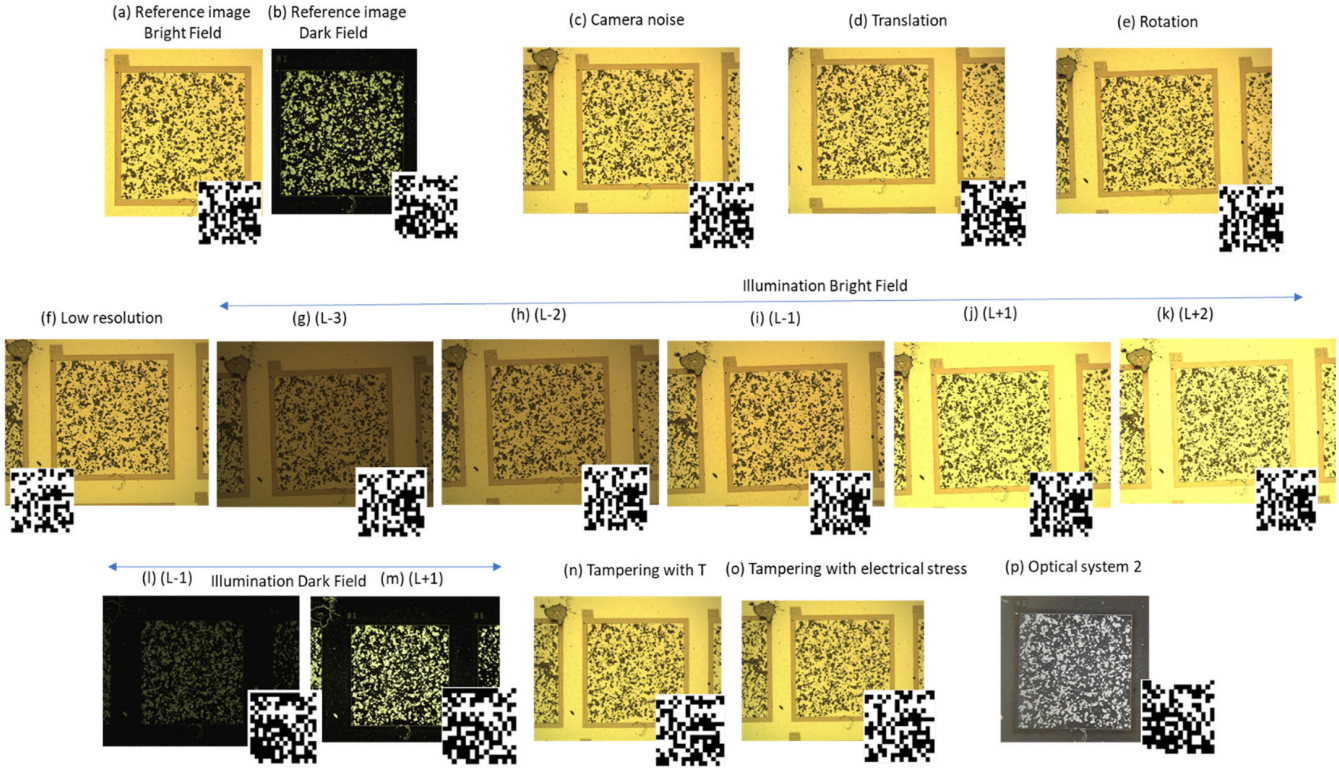

FIGURE 5. Images obtained in PUF_2 under all the different measurement conditions used in this work to evaluate the reliability of the proposed PUFs. Under each image, the obtained keys are shown. (a) and (b) correspond to the reference images taken in Bright and Dark field, respectively, to which the rest of the images will be compared. (c), (d), (e) and (f) correspond, respectively, to images taken to evaluate the impact of the camera noise, translation, rotation and resolution of the image. (g) to (m) correspond to images taken at different illuminations to evaluate its impact on the PUF reliability. (n) and (o) correspond to images taken after a temperature annealing and an electrical stress. Finally, (p) was taken with a different optical system.

TABLE 1. Mean and SD (in %) of the Uniformity after resizing, after the application of the CVN and when only considering the first 16 × 16 bits of each image after the CVN. Mean and SD of the uniqueness and Reliability when images have been translated or rotated. The camera noise and impact of resolution is also evaluated. The values have been calculated in the set of 9 PUFs.

	Uniformity (%)			Uniqueness (%)	Reliability (%)			
	After resizing	After CVN	16x16	16x16	Camera noise	Translation	Rotation	Resolution
mean	79.21	50.41	50.95	50.46	96.96	96.79	89.58	91.06
SD	12.43	1.19	2.03	2.93	2.08	1.88	3.96	3.18

and rotation, the images shown in Figs. 5c, 5d and 5e were compared with the reference image shown in Fig. 5a. The obtained key is indicated at the bottom of each image. The reliability mean value and SD measured from the 9 PUFs for the 3 cases investigated are shown in Table 1. Note that for the translated/rotated images, average reliabilities of 96.79% and 89.58% are achieved, which indicate a high degree of coincidence. For the camera noise test, higher values were found (96.96%). Fig. 6 shows the reliability histogram corresponding to the translation, rotation and camera noise test (together with the uniqueness histogram). It is worth emphasizing that, in all cases, the uniqueness histogram does not overlap with the others, which is a clear evidence that the algorithm used to select the gate area works properly, leading to high degrees of reliability.

B. DIFFERENT CONDITIONS: RESOLUTION AND ILLUMINATION

As, in practice, products are transported to different locations, images will be taken under different conditions, so a secure component identification has to be guaranteed under changing situations. In this Section, the reliability of keys obtained from pictures taken with different resolution and illumination conditions is evaluated.

1) RESOLUTION

We start evaluating the impact of using a different image resolution compared to that of the reference one on the reliability of the PUFs. Images from the 9 PUFs were obtained under identical illumination conditions and using

TABLE 2. Mean and SD reliability (in %) of the set of analyzed PUFs when 5 different illuminations are used (Bright Field), for two cases: when the same RGB thresholds were used for all the cases (RGB = 0.55/0.5/0.23) and when the RGB thresholds that maximize the reliability (obtained with a MATLAB algorithm) have been used. The mean and SD of the reliability when 2 different illuminations are used in Dark field are also shown. In this case, the developed algorithm has been used to maximize the reliability when lower (L-1) and higher (L+1) illuminations (compared to the reference image) are considered. The table also includes the reliability when different high temperature and electrical stress based attacks are simulated and when different optical systems are used to obtain the images to be compared. In the last case, optical images obtained with the optical system 2 have been compared to the reference ones, which were obtained with the optical system 1, Dark Field. CVN has been applied only in the reference image (CVN1) and in both images (CVN2).

	Illumination (%)												Tampering (%)		Optical system 2 (%)	
	Bright Field										Dark Field		Bright Field		Dark Field	
	Same RGB					Optimized RGB					Optimized RGB		Temp.	Stress	CVN1	CVN2
	L-3	L-2	L-1	L+1	L+2	L-3	L-2	L-1	L+1	L+2	L-1	L+1				
mean	49.04	72.65	94.44	90.49	86.85	94.36	94.84	95.01	95.05	94.88	90.97	94.96	95.18	96.14	84.03	98.83
SD	2.03	9.2	3.33	3.62	4.92	2.94	2.86	3.3	2.62	2.77	3.48	2.3	3.07	2.55	3.68	1.62

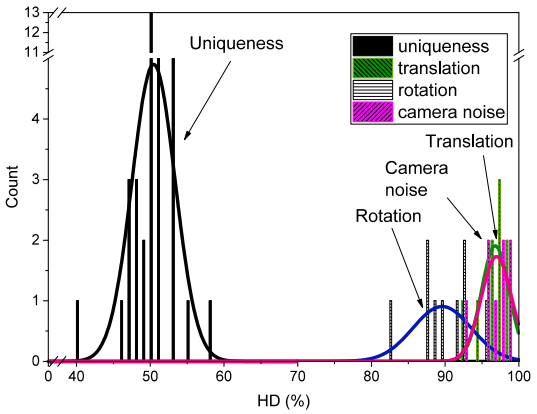

FIGURE 6. Uniqueness and reliability obtained from 9 different PUFs when the translation, rotation and camera noise test is evaluated. The average value and SD for each case are shown in Table 1.

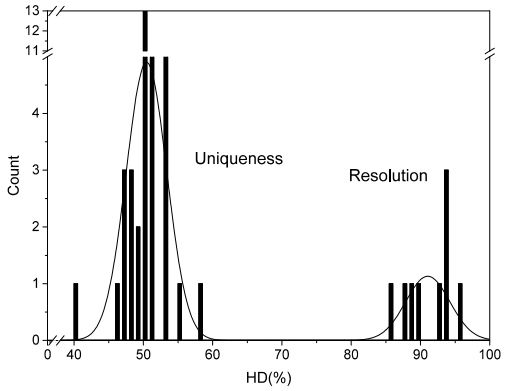

FIGURE 7. Uniqueness and reliability obtained from 9 different PUFs when the resolution test is evaluated. The average value and SD are shown in Table 1.

the same optical system employed for the reference images (without moving the sample), but with a lower resolution. While reference images were registered with a resolution of 2592 × 1944 pixels, the low-resolution images were saved with 1280 × 1024 pixels. As an example, Fig. 5f shows the low-resolution image of PUF_2, which was compared with the reference image (Fig. 5a). The low resolution images were binarized following the procedure described in Section II using the same RGB parameters (illumination conditions were not altered). Then, the intra-HD was evaluated for the 9 PUFs and the mean and SD values were computed. The corresponding key for PUF_2 is shown at the bottom of Fig. 5f. The results can also be seen in Table 1 and Fig. 7. Note that the reliability is quite high, reaching a mean value of 91.06% in terms of coincidence. Fig. 7 shows the histogram corresponding to low resolution images together with the uniqueness histogram. Again, the separation of the two histograms indicates a high degree of reliability of the proposed PUFs.

2) ILLUMINATION

Illumination is also a critical issue when assessing the reliability of the proposed PUFs. While all *reference* images (those stored in the database) can be taken under identical illumination conditions and binarized using the same RGB values, during the authentication stage, potential users will take pictures of the PUFs with an illumination that will hardly coincide with the reference one. Therefore, when using the same RGB values as those used in the prestored images, the PUFs reliability could be seriously affected. For this reason, this issue must be addressed carefully.

We analyzed the impact of the illumination conditions for two different cases: when images are taken in (i) Bright Field and in (ii) Dark Field. For the Bright Field case, images taken with 5 different illuminations from the reference one have been registered for the 9 PUFs (Figs. 5g-k). For the sake of clarity, the images taken under different illuminations are referred to as (L-3), (L-2), (L-1), (L+1) and (L+2). Note that for 3 out of the 5 cases considered (the first 3 cases), the illumination is lower than that used for the reference image, while for 2 cases, that is, for the case (L+1) and (L+2), the illumination is higher. The illumination of the reference image is in between cases (L-1) and (L+1). Note that the images presented in Figures 5g–5k show a wide

range of lighting conditions, from very poor illumination (Figure 5g) to overexposed images with excessive lighting (Figure 5k). This range was intentionally selected to reflect realistic and extreme variations in lighting and to ensure that the performance of the PUFs is robust across these conditions. Table 2 shows the mean value and SD of the 9 PUFs reliability obtained when comparing these 5 images with the reference ones. First, the RGB thresholds for both images, the reference one and that taken by the potential user, are the same, i.e. RGB = 0.55/0.5/0.23. Note that, for the cases (L-1) and (L+1), the reliability is quite high (since the illumination is quite similar to the reference case), reaching an average value of 94.44% and 90.49%, respectively. However, when the illumination notably differs, the reliability decreases, reaching unacceptable values, as occurs in the (L-3) case for instance, where the mean value is 49.04%. In summary, when the illumination used to take the images is quite different, to carry out a fair binarization, the RGB thresholds cannot be identical.

In order to overcome this important limitation, we developed a MATLAB routine to this end. While for the reference images the same values of RGB can always be used, for the alternative images, different RGB thresholds must be considered to optimize the reliability of the PUF. To obtain the values that maximize this feature, first, the 'B' threshold is scanned in a given range and with a given step (usually from 0.05 to 0.95, with a step of 0.02), while keeping R and G constant, with values 0.4 and 0.3 (initial values that are suitable even for very dark images, as in the case L-3). Then, the 'B' threshold is set to the value that maximizes the reliability, R = 0.4 and the 'G' threshold is scanned in a similar fashion as 'B' (in the range of 0.05-0.95, with a step of 0.05). Finally, as for the 'B' threshold, the 'G' threshold is set to the value that maximizes the reliability, and R is scanned in the same range of 'G' and with the same step. The RGB thresholds that maximize the reliability of each PUF (which can change from PUF to PUF) are then considered for the evaluation of the reliability of individual PUFs. For illustrative purposes, Figs. 5g-k show the keys obtained in each case for PUF_2. Table 2 shows the mean and SD value of the reliability of the analyzed PUFs following this procedure. Note that the obtained reliability shows a high degree of coincidence (∼95% in all cases) and is higher when compared to the case in which the same thresholds were used for both images. This is especially true when images obtained with very different illuminations are compared. Fig. 8 shows the reliability histogram corresponding to images registered at different illuminations (for clarity, only (L+1) and (L-3) are shown, together with the uniqueness histogram). Again, the uniqueness and reliability histograms do not overlap, indicating a high degree of reliability of the proposed PUFs.

The same MATLAB algorithm used for the optimization of the RGB thresholds was also applied to images taken in Dark Field. In particular, images taken under lower (L-1) and higher (L+1) different illumination from that of the reference were registered (Fig. 5l-m, for PUF_2, which also shows the obtained key). The reliability mean and SD of the 9 PUFs set is shown in Table 2. Note again that the reliability factor shows a high degree of coincidence (90-95%), demonstrating that the methodology proposed here to evaluate the reliability of PUFs when different illuminations are used provides good results.

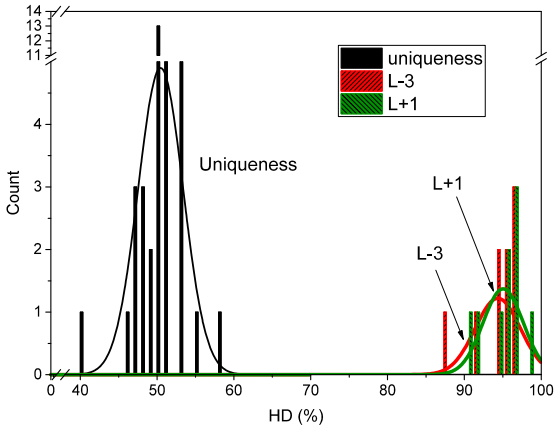

FIGURE 8. Uniqueness and reliability obtained from 9 different PUFs when the illumination impact is evaluated in Bright Field. Only case (L+1) and (L-3) are shown for clarity. The average value and SD for each case are shown in Table 2.

C. TAMPERING: ELECTRICAL STRESS AND ANNEALING ATTACKS

Tampering is also a very important issue when dealing with PUFs. An ideal PUF should be resistant to tampering and, if possible, also indicate the tampering attempt [39], [40], [41]. In this Section, we simulate two kinds of attacks. First, we tested the proposed PUFs against changes in temperature associated with variations of the ambient conditions and/or because of attacks consisting in high temperature processes. Second, we evaluate the PUFs when subjected to additional electrical stress. In both cases, since images were obtained in different days and with different illuminations, the algorithm reported in section B was used to select the RGB threshold that optimizes the reliability of the PUF.

1) TEMPERATURE VARIATIONS

To evaluate the impact of changes of temperature on the PUFs, the PUFs were subjected to a 150 °C annealing during 25 minutes. Then, the fingerprints of the 9 PUFs obtained after the annealing were compared with those corresponding to images registered before the annealing (that is, the reference image) to evaluate the reliability of the PUF. For PUF_2, Fig. 5n was compared to Fig. 5a. The reliability mean and SD obtained from the 9 analyzed PUFs are reported in Table 2, being 95.18% and 3.07%, respectively, which indicate a high degree of coincidence. Therefore, the obtained results indicate that the proposed PUFs are resilient to attacks consisting in temperature annealings.

2) ELECTRICAL STRESSES ATTACKS

The investigated PUFs were also tested under electrical stress. Since the proposed PUFs are inherently the consequence of electrical stress, it is important to assess whether they can be significantly altered or not by the action of additional electrical stresses. Otherwise, they could be altered using the same process with which they were generated. To evaluate the impact of electrical attacks, an additional stress of −14V (Current Limit of 0.1A) for 180s was applied to the 9 PUFs. After the stress, the fingerprints were compared with those corresponding to images obtained before the attack, namely, the reference images (i.e., Fig. 5o was compared to Fig. 5a). The mean value is 96.14% (see Table 2), which indicates, once again, that a high degree of coincidence is achieved. Fig. 9 shows that the uniqueness histogram does not overlap with the reliability histograms obtained after the simulated attacks, demonstrating that the proposed PUFs are resilient to attacks based on temperature and electrical stresses.

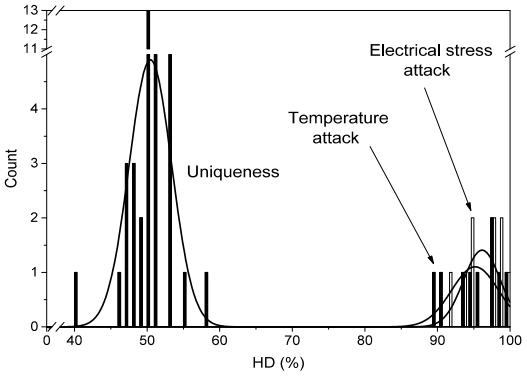

FIGURE 9. Uniqueness and reliability obtained from 9 different PUFs when the temperature and electrical stress attacks were simulated. The average value and SD for each case are shown in Table 2.

D. THE ROLE OF THE OPTICAL SYSTEM

As products are transported to different locations, different optical systems will likely record the images, so secure component identification has to be guaranteed under these circumstances. In this Section, to emulate a real case, images taken by a potential user were obtained with a different optical system to that considered for the reference images (which will be stored in the database). In this case, images were obtained with the *optical system 2,* which consists of a low cost optical Microscope (Swift SW100), Dark Field (with a magnification of 10×10) plus a mobile phone to register the images. In particular, the images were registered with a standard Samsung Galaxy A50 with 3024×4032 pixels resolution. The images were taken with a digital zoom of 3.1. After the selection of the gate area, the reliability was evaluated by comparing the fingerprint obtained with the *optical system 2* (Fig. 5p) with that obtained from the reference images (registered with the *optical system 1*, Fig. 3 right and 5b). Table 2 (column CVN1) shows the reliability mean and SD value obtained from the 9 PUFs when CVN is exclusively applied to the reference image (as in all previous cases). Note that the reliability factor is high (average = 84.03%) though somewhat lower than in the previous analysis. However, note that the uniqueness histogram does not overlap with the reliability one (Fig. 10), suggesting that the result is good enough to reproduce the fingerprints unambiguously. However, we tried to improve the reliability values by applying the CVN to both images (Table 2, column CVN2). In this case, since bits from both images are ruled out, only those bits which were not eliminated in both images were considered for the evaluation of the intra-HD. When CVN is applied to both images, the results improve in terms of reliability, with a mean value of 98.83%. Fig. 10 shows that the uniqueness and reliability histograms for these cases do not overlap, showing that the proposed PUFs meet the expected requirements when different optical systems are used.

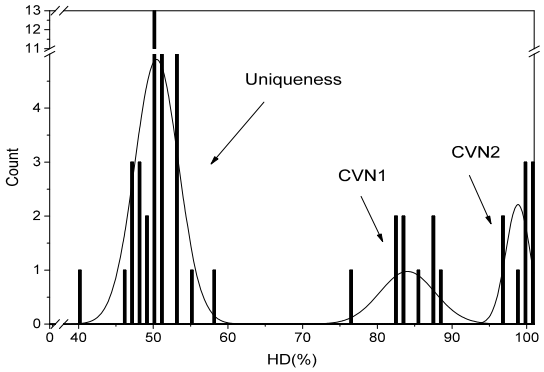

FIGURE 10. Uniqueness and reliability histograms obtained from 9 different PUFs when different optical systems are used to get the images, when CVN is applied to the reference image only (CVN1), or to both images (CVN2). The average and SD values for each case are shown in Table 2.

TABLE 3. Degree of coincidence (in %) between an image taken in a fake capacitor (case A') and an image of PUF_2 taken with very bad illumination conditions and rotation (case B´), with the reference images of all the 9 PUFs of our *database*. The images (Bright Field) are shown in Fig. 11 (top). Only case B', which corresponds to a non-fake PUF, shows a high degree of coincidence when it is compared with the reference image of PUF_2 (shadowed), as expected.

degree of coincidence (BRIGHT FIELD)		
	A' : FAKE IMAGE	B' : IMAGE taken on PUF_2
	CVN	CVN
PUF_1	45,7	55,07
PUF_2	52,73	92,58
PUF_3	55,47	53,9
PUF_4	52,73	52,73
PUF_5	54,97	49,6
PUF_6	51,95	53,12
PUF_7	55,86	50,78
PUF_8	53,91	54,3
PUF_9	55,47	51,56

TABLE 4. Degree of coincidence (in %) between the images taken for cases A and B (fake capacitors) and for cases C and D (PUF_7 and PUF_2) with all the 9 PUF's images in our database. The images (Dark mode) are shown in Fig. 11. The degree of coincidence has been evaluated by applying CVN in the reference image only (CVN1) and in both images (CVN2). Only cases C and D, which correspond to non-fake PUFs, show a high degree of coincidence when they are compared with the reference image of PUF_7 and PUF_2 (shadowed), respectively, as expected.

degree of coincidence (DARK FIELD, DIFFERENT OPTICAL SYSTEMS)								
	A: FAKE IMAGE		B: FAKE IMAGE		C: Image taken on PUF_7		D: Image taken on PUF_2	
	CVN1	CVN2	CVN1	CVN2	CVN1	CVN2	CVN1	CVN2
PUF_1	53,51	54,3	53,13	48,83	51,95	50,39	51,17	49,22
PUF_2	51,95	53,9	51,95	51,17	52,73	54,68	87,11	99,61
PUF_3	56,25	53,52	56,25	50,78	56,64	51,56	58,59	54,69
PUF_4	51,95	58,97	50,34	49,61	51,95	54,69	51,95	48.13
PUF_5	51,56	55,47	51,95	47,66	52,73	52,73	53,51	53,51
PUF_6	52,34	52,73	58,03	49,22	51,17	54,3	53,51	55,08
PUF_7	53,12	49,77	52,73	47,65	88,28	100	51,95	49,77
PUF_8	54,3	56,64	55,08	52,73	53,13	48,83	51,95	53,13
PUF_9	52,73	48,44	51,56	51,95	56,25	51,56	54,3	53,52

In conclusion, the results shown in Section IV demonstrate that, despite changes in the conditions of the image registration or tampering attempts, the proposed PUFs show high levels of reliability, ranging from ∼90 to ∼99% (depending on the aspect considered), which are comparable to those found in other previously proposed PUFs based on images, as those shown in [28] and [32] (∼95%). Similar or higher values of reliabilities (∼97-100%) can be found on other PUFs based on post-BD currents [21], [42], but in this case, additional circuitry is necessary for the current measurement and in [22] it is reported that they can be vulnerable to physical inspection attacks. Therefore, the PUF key can be more easily extracted. Moreover, it is important to take into account that different methods could be applied to improve even more the reliability of the PUFs. For example, the bit flipping problem [43] (i.e., bits that change due to the different conditions used to obtain a bit of a PUF), can be corrected by introducing Error Correction Codes (ECCs) [44], or by bit selection (that is, selecting the most reliable bits [45]).

V. EMULATION OF THE AUTHENTICATION STAGE

Finally, in this Section, an emulation of a real authentication process is reported. For the sake of completeness, different cases are considered i.e., fake and non-fake PUFs, bright and dark field mode acquisitions and different optical systems. The obtained images were compared to those contained in the database taken with the optical system 1, which includes images of the 9 PUFs (PUF_1 to PUF_9) in Bright and Dark Fields, shown in Fig. 3. First, cases A´and B´were analyzed, whose associated images were taken with the *optical system 1* in the Bright field mode and are shown in Fig. 11 (top). Case A' corresponds to a fake PUF (not registered in the database) and case B' corresponds to PUF_2. In the last case, however, the image was taken under very bad illumination conditions and with a certain rotation. Second, cases A and B were evaluated, whose images were taken in the Dark field mode with *optical system 2* and are shown in Fig. 11 (middle). These cases correspond to fake PUFs, taken by users that purchased a fake product (the images do not correspond to

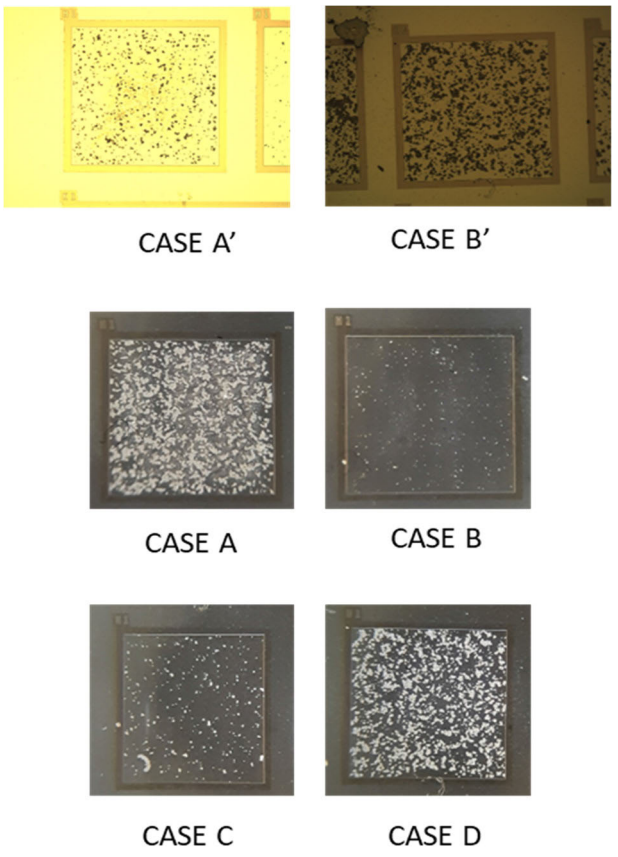

FIGURE 11. CASE A': Image of a fake PUF, i.e., of a capacitor whose image is not stored in the database. CASE B': Image of PUF_2 taken in very bad illumination conditions and some rotation. Both images were taken with optical system 1 in Bright field mode. CASE A and B are fake images and CASE C and D correspond to images taken, respectively from PUF_7 and PUF_2, all with the optical system 2 in Dark Field.

any of the images stored in the database). To take into account extreme possible situations, case B corresponds to an image with few BD spots while case A to a capacitor with a high density of spots. Finally, two cases of non-fake capacitors are also considered, whose images were taken with *optical system 2* in Dark field mode (Fig. 11, bottom): case C, with only a few spots, and D with a large number of spots, which correspond to products that were purchased with PUF_7 and PUF_2, respectively. The images in Fig. 11 are compared to all those stored in the database and the degree of coincidence has been evaluated from the intra-HD, which is shown in Tables 3 and 4, for the Bright Field and Dark Field cases, respectively. For those images taken in the Dark Field mode, the comparison was performed under two circumstances: when the CVN is exclusively applied to the reference image (CVN1), and when it is applied both to the reference image and to that taken by the user (CVN2).

Note that, in cases A', A and B (which correspond to fake PUFs), the intra-HD always shows a degree of coincidence ranging from 45.7% to 58.97% (see Table 3 and 4), which is very low, suggesting, as expected, that the product is fake. On the other hand, in the case of the images of real PUFs, i.e., cases B', C and D, the degree of coincidence is very low when the images are compared to those obtained in other PUFs, but it is high when they are compared to those in the database for the same PUF (PUF_2 and PUF_7). In particular, a reliability of 92.58% is obtained for Case B' (Table 3), and values of 88.28%/100% and 87.11%/99.61% are found for CVN1/CVN2 in cases C and D, respectively (Table 4), demonstrating that the product is not fake. The emulation of these cases shows that the proposed devices fully meet the reliability requirements for their use as PUFs.

VI. CONCLUSION

In summary, the reliability of a new approach for the generation of PUFs, based on catastrophic breakdown spot spatial patterns electrically generated in MIM structures and optically recorded, was assessed. The obtained results demonstrate that the generated fingerprints meet the essential requirements of uniformity, uniqueness and reliability. Because of its utmost importance, this last issue was evaluated in detail. We have assessed different aspects of the key verification problem, such as the selection of the gate area of the device to be analysed (which is crucial to compare the images obtained by the final user with the one stored in the database), the effect of the image resolution, the illumination conditions, the noise introduced by the camera setup, and the use of different optical systems for reference and user image generation. It was shown that the algorithm used to select the gate area is able to compensate undesired translations or rotations of the images so that a fair comparison can be made. For illumination compensation, we developed a routine in MATLAB that allows comparing images taken under different illumination conditions. In all cases, the solutions proposed in this work allow achieving a high degree of coincidence when different images of the same capacitor taken under different conditions are compared. This translates into high reliability which can reach values up to ∼90 or ∼99% depending on the analysed scenario. Finally, several key reading real situations were emulated. Images taken on fake capacitors (not registered in the database) and others taken on PUFs stored in the database were compared with all the reference images available. The degree of coincide of all fake capacitors was found to be very poor, as expected. Only non-fake PUFs, gave a high degree of coincidence when compared with the reference image of the same PUF. The investigated PUFs are also resilient to attacks based on temperature and electrical stresses, as opposed to other CMOS-PUFs relying on the electrical properties of devices and/or circuits vulnerable to such attacks. Notice that the proposed approach does not require extra circuitry as many other systems do, notably reducing the associated cost and complexity. Only an adequate test set-up is necessary to stress the devices until BD to generate the PUFs (but this can be done beforehand in a specialized laboratory) and a low-cost optical system for image recording at the customer site. Importantly, the proposed PUF is fully compatible with the conventional manufacturing technology of MIM and MIS devices.

ACKNOWLEDGMENT

The authors would like to thank Dr. P. Hurley from the Tyndall National Institute, Ireland, for sample provision and G. Abadal from UAB for making available the optical system.

REFERENCES

[1] J. Suñé, 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, Mar. 1990, doi: 10.1016/0040-6090(90)90098-x.

[2] K. Shubhakar, K. L. Pey, N. Raghavan, S. S. Kushvaha, M. Bosman, Z. Wang, and S. J. O'Shea, "Study of preferential localized degradation and breakdown of HfO_2/SiO_x dielectric stacks at grain boundary sites of polycrystalline HfO_2 dielectrics," *Microelectron. Eng.*, vol. 109, pp. 364–369, Sep. 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, no. 19, Nov. 2012, Art. no. 193502, doi: 10.1063/1.4765342.

[4] U. Celano, Y. Yin 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, Mar. 2013, Art. no. 121602, doi: 10.1063/1.4798525.

[5] Y.-L. Wu, J.-J. Lin, B.-T. Chen, and 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, Mar. 2012, doi: 10.1109/TDMR.2011.2179804.

[6] M. Porti, S. Meli, M. Nafría, and X. Aymerich, "New insights on the post-BD conduction of MOS devices at the nanoscale," *IEEE Electron Device Lett.*, vol. 26, no. 2, pp. 109–111, Feb. 2005, doi: 10.1109/LED.2004.841190.

[7] M. Porti, M. Nafria, and X. Aymerich, "Current limited stresses of SiO_2 gate oxides with conductive atomic force microscope," *IEEE Trans. Electron Devices*, vol. 50, no. 4, pp. 933–940, Apr. 2003, doi: 10.1109/TED.2003.812082.

[8] S. Claramunt, Q. Wu, M. Maestro, M. Porti, M. B. Gonzalez, J. Martin-Martinez, F. Campabadal, and M. Nafría, "Non-homogeneous conduction of conductive filaments in $Ni/HfO_2/Si$ resistive switching structures observed with CAFM," *Microelectron. Eng.*, vol. 147, pp. 335–338, Nov. 2015, doi: 10.1016/j.mee.2015.04.112.

[9] M. Porti, M. Nafría, M. C. Blüm, X. Aymerich, and S. Sadewasser, "Atomic force microscope topographical artifacts after the dielectric breakdown of ultrathin SiO_2 films," *Surf. Sci.*, vols. 532–535, pp. 727–731, Jun. 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, and 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, Jun. 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–HfO_2–Si resistive-switching operational devices," *Appl. Phys. Exp.*, vol. 11, no. 1, Jan. 2018, Art. no. 014101, doi: 10.7567/apex.11.014101.

[12] J. Muñoz-Gorriz, S. Monaghan, K. Cherkaoui, J. Suñé, P. K. Hurley, and E. Miranda, "Exploratory study and application of the angular wavelet analysis for assessing the spatial distribution of breakdown spots in Pt/HfO_2/Pt structures," *J. Appl. Phys.*, vol. 122, no. 21, Dec. 2017, Art. no. 215304, doi: 10.1063/1.5000004.

[13] J. Muñoz-Gorriz, S. Monaghan, K. Cherkaoui, J. Suñé, P. K. Hurley, and 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, May 2018, doi: 10.1007/s11664-018-6298-2.

[14] N. Liu, N. Pinckney, S. Hanson, D. Sylvester, and D. Blaauw, "A true random number generator using time-dependent dielectric breakdown," in *Symp. VLSI Circuits-Dig. Tech. Papers*, Jun. 2011, pp. 216–217.

[15] S. Yasuda, H. Satake, T. Tanamoto, R. Ohba, K. Uchida, and S. Fujita, "Physical random number generator based on MOS structure after soft breakdown," *IEEE J. Solid-State Circuits*, vol. 39, no. 8, pp. 1375–1377, Aug. 2004, doi: 10.1109/JSSC.2004.831480.

[16] J.-W. Nam, J.-H. Ahn, and J.-P. Hong, "Compact SRAM-based PUF chip employing body voltage control technique," *IEEE Access*, vol. 10, pp. 22311–22319, 2022, doi: 10.1109/ACCESS.2022.3153359.

[17] N. N. Anandakumar, M. S. Hashmi, and M. A. Chaudhary, "Implementation of efficient XOR arbiter PUF on FPGA with enhanced uniqueness and security," *IEEE Access*, vol. 10, pp. 129832–129842, 2022, doi: 10.1109/ACCESS.2022.3228635.

[18] Y. Shifman, A. Miller, O. Keren, Y. Weizman, and J. Shor, "A method to utilize mismatch size to produce an additional stable bit in a tilting SRAM-based PUF," *IEEE Access*, vol. 8, pp. 219137–219150, 2020, doi: 10.1109/ACCESS.2020.3042092.

[19] Y. Pang, H. Wu, B. Gao, N. Deng, D. Wu, R. Liu, S. Yu, A. Chen, and H. Qian, "Optimization of RRAM-based physical unclonable function with a novel differential read-out method," *IEEE Electron Device Lett.*, vol. 38, no. 2, pp. 168–171, Feb. 2017, doi: 10.1109/LED.2016.2647230.

[20] D. Kim, T.-H. Kim, Y. Choi, G. H. Lee, J. Lee, W. Sun, B.-G. Park, H. Kim, and H. Shin, "Selected bit-line current PUF: Implementation of hardware security primitive based on a memristor crossbar array," *IEEE Access*, vol. 9, pp. 120901–120910, 2021, doi: 10.1109/ACCESS.2021.3108534.

[21] K.-H. Chuang, E. Bury, R. Degraeve, B. Kaczer, D. Linten, and I. Verbauwhede, "A physically unclonable function using soft oxide breakdown featuring 0% native BER and 51.8 fJ/bit in 40-nm CMOS," *IEEE J. Solid-State Circuits*, vol. 54, no. 10, pp. 2765–2776, Oct. 2019, doi: 10.1109/JSSC.2019.2920714.

[22] P. Saraza-Canflanca, F. Fodor, J. Diaz-Fortuny, B. Gierlichs, R. Degraeve, B. Kaczer, I. Verbauwhede, and E. Bury, "Unveiling the vulnerability of oxide-breakdown-based PUF," *IEEE Electron Device Lett.*, vol. 45, no. 5, pp. 750–753, May 2024, doi: 10.1109/LED.2024.3369860.

[23] K.-H. Chuang, E. Bury, R. Degraeve, B. Kaczer, T. Kallstenius, G. Groeseneken, D. Linten, and I. Verbauwhede, "A multi-bit/cell PUF using analog breakdown positions in CMOS," in *Proc. IEEE Int. Rel. Phys. Symp. (IRPS)*, Mar. 2018, pp. P-CR.2-1–P-CR.2-5, doi: 10.1109/IRPS.2018.8353655.

[24] N. A. Anagnostopoulos, T. Arul, M. Rosenstihl, A. Schaller, S. Gabmeyer, and S. Katzenbeisser, "Low-temperature data remanence attacks against intrinsic SRAM PUFs," in *Proc. 21st Euromicro Conf. Digit. Syst. Design (DSD)*, Prague, Czech Republic, Aug. 2018, pp. 581–585, doi: 10.1109/DSD.2018.00102.

[25] A. Douadi, G. Di Natale, P. Maistri, E.-I. Vatajelu, and V. Beroulle, "A study of high temperature effects on ring oscillator based physical unclonable functions," in *Proc. IEEE 29th Int. Symp. On-Line Test. Robust Syst. Design (IOLTS)*, Chania, Greece, Jul. 2023, pp. 1–7.

[26] A. Cathignol, B. Cheng, D. Chanemougame, A. R. Brown, K. Rochereau, G. Ghibaudo, and A. Asenov, "Quantitative evaluation of statistical variability sources in a 45-nm technological node LP N-MOSFET," *IEEE Electron Device Lett.*, vol. 29, no. 6, pp. 609–611, Jun. 2008, doi: 10.1109/LED.2008.922978.

[27] T. Kroeger, W. Cheng, S. Guilley, J.-L. Danger, and N. Karimi, "Effect of aging on PUF modeling attacks based on power side-channel observations," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2020, pp. 454–459, doi: 10.23919/DATE48585.2020.9116428.

[28] J. W. Leem, M. S. Kim, S. H. Choi, S.-R. Kim, S.-W. Kim, Y. M. Song, R. J. Young, and Y. L. Kim, "Edible unclonable functions," *Nature Commun.*, vol. 11, no. 1, p. 328, Jan. 2020, doi: 10.1038/s41467-019-14066-5.

[29] A. T. Erozan, M. Hefenbrock, D. R. E. Gnad, M. Beigl, J. Aghassi-Hagmann, and M. B. Tahoori, "Counterfeit detection and prevention in additive manufacturing based on unique identification of optical fingerprints of printed structures," *IEEE Access*, vol. 10, pp. 105910–105919, 2022, doi: 10.1109/ACCESS.2022.3209241.

[30] B. Wigger, T. Meissner, A. Förste, V. Jetter, and A. Zimmermann, "Using unique surface patterns of injection moulded plastic components as an image based physical unclonable function for secure component identification," *Sci. Rep.*, vol. 8, no. 1, p. 4738, Mar. 2018, doi: 10.1038/s41598-018-22876-8.

[31] B.-H. Wu, C. Zhang, N. Zheng, L.-W. Wu, Z.-K. Xu, and 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, Dec. 2018, doi: 10.1021/acsapm.8b00031.

[32] N. Torun, I. Torun, M. Sakir, M. Kalay, and M. S. Onses, "Physically unclonable surfaces via dewetting of polymer thin films," *ACS Appl. Mater. Interfaces*, vol. 13, no. 9, pp. 11247–11259, Feb. 2021, doi: 10.1021/acsami.0c16846.

[33] Z. Chi, A. Valehi, H. Peng, M. Kozicki, and A. Razi, "Consistency penalized graph matching for image-based identification of dendritic patterns," *IEEE Access*, vol. 8, pp. 118623–118637, 2020, doi: 10.1109/ACCESS.2020.3005184.

[34] F. Peng, J. Yang, and M. Long, "3-D printed object authentication based on printing noise and digital signature," *IEEE Trans. Rel.*, vol. 68, no. 1, pp. 342–353, Mar. 2019, doi: 10.1109/TR.2018.2869303.

[35] M. Porti, M. Redón, J. Muñoz, M. Nafría, and E. Miranda, "Oxide breakdown spot spatial patterns as fingerprints for optical physical unclonable functions," *IEEE Electron Device Lett.*, vol. 44, no. 10, pp. 1600–1603, Oct. 2023, doi: 10.1109/LED.2023.3301974.

[36] C. D. Kuglin and D. C. Hines, "The phase correlation image alignment method," in *Proc. IEEE Int. Conf. Cybern. Soc.*, San Francisco, CA, USA, Sep. 1975, pp. 163–165.

[37] B. S. Reddy and B. N. Chatterji, "An FFT-based technique for translation, rotation, and scale-invariant image registration," *IEEE Trans. Image Process.*, vol. 5, no. 8, pp. 1266–1271, Aug. 1996, doi: 10.1109/83.506761.

[38] R. Maes, V. van der Leest, E. van der Sluis, and F. Willems, "Secure key generation from biased PUFs: Extended version," *J. Cryptograph. Eng.*, vol. 6, no. 2, pp. 121–137, Mar. 2016, doi: 10.1007/s13389-016-0125-6.

[39] B. R. Anderson, R. Gunawidjaja, and H. Eilers, "Initial tamper tests of novel tamper-indicating optical physical unclonable functions," *Appl. Opt.*, vol. 56, no. 10, p. 2863, 2017, doi: 10.1364/ao.56.002863.

[40] B. P. Williams, K. A. Britt, and T. S. Humble, "Tamper-indicating quantum seal," *Phys. Rev. Appl.*, vol. 5, no. 1, Jan. 2016, Art. no. 014001, doi: 10.1103/physrevapplied.5.014001.

[41] J.-L. Danger, S. Guilley, M. Pehl, S. Senni, and Y. Souissi, "Highly reliable PUFs for embedded systems, protected against tampering," in *Industrial Networks and Intelligent Systems* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 379, N. S. Vo, V. P. Hoang, and Q. T. Vien, Eds., Cham, Switzerland: Springer, 2021, pp. 167–184, doi: 10.1007/978-3-030-77424-0_14.

[42] M.-Y. Wu, T.-H. Yang, L.-C. Chen, C.-C. Lin, H.-C. Hu, F.-Y. Su, C.-M. Wang, J. P. Huang, H.-M. Chen, C. C. Lu, E. C. Yang, and R. S. Shen, "A PUF scheme using competing oxide rupture with bit error rate approaching zero," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, San Francisco, CA, USA, Feb. 2018, pp. 130–132, doi: 10.1109/ISSCC.2018.8310218.

[43] I. Baturone, M. A. Prada-Delgado, and S. Eiroa, "Improved generation of identifiers, secret keys, and random numbers from SRAMs," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2653–2668, Dec. 2015, doi: 10.1109/TIFS.2015.2471279.

[44] 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, Jun. 2018, Art. no. 9653, doi: 10.1038/s41598-018-28008-6.
[45] A. Santana-Andreo, P. Saraza-Canflanca, H. Carrasco-Lopez, P. Brox, R. Castro-Lopez, E. Roca, and F. V. Fernandez, "A DRV-based bit selection method for SRAM PUF key generation and its impact on ECCs," *Integration*, vol. 85, pp. 1–9, Jul. 2022, doi: 10.1016/j.vlsi.2022.02.008.

MARC PORTI (Member, IEEE) received the Ph.D. degree from Universitat Autònoma de Barcelona (UAB), Spain, in 2003. In 1998, he joined the Department of Electronic Engineering, UAB, where he is currently an Associate Professor. He studied the reliability and impact of radiation in SiO2 and high-k gate dielectrics. Recently, the variability and reliability of nanoelectronic and emergent devices have been topics of his interest, for example RRAM devices and devices based on 2D materials, such as graphene and organic materials. His research interests include applications of scanning probe microscopies for the nanoscale electrical characterization of gate oxides nanoelectronic devices.

ALVARO SOLIS received the degree in telecommunications engineering from Universitat Autònoma de Barcelona (UAB), Barcelona, Spain, in 2024, where he is currently pursuing the master's degree in telecommunications engineering. In 2023, he joined the Electronic Engineering Department, UAB, to work on the application of breakdown spot spatial distribution for PUFs applications.

ALEX CALATAYUD received the degree in telecommunications engineering from Universitat Autònoma de Barcelona (UAB), Barcelona, Spain, in 2023. In 2022, he joined the Electronic Engineering Department, UAB, working on the application of breakdown spot spatial distribution for PUFs applications.

MONTSERRAT NAFRÍA (Senior Member, IEEE) is currently a Full Professor with the Department of Electronic Engineering, Universitat Autònoma de Barcelona (UAB), Barcelona, Spain, where she is involved in the characterization and modeling of the time-dependent variability of advanced MOS devices, to develop models for circuit reliability simulators. She is also interested in resistive RAM and graphene-based devices. She has co-authored more than 250 research papers in scientific journals and conferences in these fields.

ENRIQUE MIRANDA (Senior Member, IEEE) received the Ph.D. degree in electronics engineering from Universitat Autònoma de Barcelona (UAB), Spain, in 1999, and the Ph.D. degree in physics from Universidad de Buenos Aires, Argentina, in 2001. He was a Visiting Scientist at Indian Institute of Technology, Technical University Darmstadt, IHP, Universita di Napoli, Modena, Cagliari, and Soochow University. He is currently a Professor with UAB. He has authored and co-authored around 300 peer-reviewed journal articles most of them devoted to the electron transport mechanisms in thin dielectric films. He received numerous scholarships and awards, including INTERCAMPUS, Universidad de Zaragoza, Spain; MUTIS, UAB; RAMON y CAJAL, UAB; DAAD, Technical University Hamburg-Harburg; Italian Government, Universita degli Studi di Padova; MATSUMAE, Tokyo Institute of Technology, Japan; TAN CHIN TUAN, Nanyang Technological University, Singapore; the WALTON Award from the Science Foundation Ireland, Tyndall National Institute, the Distinguished Visitor Award from the Royal Academy of Engineering, U.K., the CESAR MILSTEIN, CNEA, Argentina; and Visiting Professorships from the Abdus Salam International Centre for Theoretical Physics; Slovak Academy of Sciences; Politecnico di Torino; Leverhulme Trust, University College London, U.K.; and the Nokia Foundation, University of Turku, Finland. He has been serving as a member of the Distinguished Lecturer Program of the Electron Devices Society (EDS-IEEE), since 2001.