Received 8 December 2021; revised 27 January 2022; accepted 31 January 2022. Date of publication 7 February 2022; date of current version 22 February 2022.
The review of this article was arranged by Editor S. Ikeda.

Digital Object Identifier 10.1109/JEDS.2022.3149321

Fabrication and Characterization of 2-Bit per Capacitor as Functional Structures for Physical Unclonable Function Circuits

J. BIBA, S. BOCHE, U. GOβNER, AND W. HANSCH

Institute of Physics, Department of Electrical Engineering and Information Technology, Universität der Bundeswehr München, 85579 Neubiberg, Germany

CORRESPONDING AUTHOR: J. BIBA (e-mail: josef.biba@unibw.de)

This work was support by the FORscience Research Fund of the Universität der Bundeswehr München.

ABSTRACT Currently, security issues for semiconductor chips are counterfeiting and night shift problems. These factors might lead to insecure supply chains in the automotive industry. This can be avoided by using coating Physical Unclonable Functions (PUFs). The coating can be applied to every semiconductor chip in order to create a unique fingerprint. In this work, a 2-bit key per capacitor for Physical Unclonable Functions is presented for the first time. For this reason, 49 chips on a wafer with 195 metal oxide semiconductor (MOS) capacitors were fabricated. A large and random fluctuation of the capacitances was achieved by using a self-developed layer, which consisted of aluminum particles and spin-on glass. Due to the random variation in size and change in distribution of the particles, the fluctuation of capacitance varied from chip to chip and from wafer to wafer. The achieved large range in capacitance was used to create a 390-bit string out of 195 capacitors. Although the length of the bit string was doubled, the area of the structure remained constant. This led to a more secure PUF with a low error rate of 0.21% and an inter-chip Hamming distance (HD_{inter}) of 49%.

INDEX TERMS Coating PUF, electrical measurement, MOS capacitors, physical unclonable functions.

I. INTRODUCTION

The Internet of Things (IoT) and the automotive sector are two end-user markets with rising growth rates for the semiconductor industry. In the IoT, smart devices are connected with each other. This leads to a high amount of secured data. Security of these data is achieved by using bit strings as cryptographic keys. These are stored in a non-volatile memory. However, not all semiconductor chips possess an included memory. This disadvantage leads to the development of Physical Unclonable Functions (PUF). In this case, the unavoidable minimal random physical fluctuations that occur through processing the semiconductor chip are used to generate the cryptographic key. These physical disorders vary from chip to chip and ideally make the PUF unclonable [1].

A lot of research has been conducted on PUFs, which use existing functional blocks on the silicon chip. The most common examples are: static random-access memory (SRAM) [2], [3], [4], ring oscillators [5], [6], [7], and arbiter PUFs [8], [9], [10]. However, not all fabricated silicon chips have these functional blocks in their layout. For example, sensors and discrete devices cannot be secured that way without a high cost rise and a large additional chip area. For instance, the automotive industry is currently developing an interest in securing these chips, as well. This industry has been going through many changes in the last years. Car connectivity, autonomous driving, and electric mobility are causing automotive companies to become more dependent on the semiconductor industry. Due to liability reasons, the automotive industry requires secure supply chains. This may be achieved by using certified and identifiable chips [11], [12]. To accomplish this goal, coating PUFs seem to be a good solution [13], [14], [15]. These PUFs consist of a particle layer, which is spun on the chip and causes a change in the electrical readout. The fingerprint is then generated by using a bit string. This is created by a pattern of capacitors.

The typical design of a coating PUF is the so-called comb structure [13]. This is covered by a particle layer, which may cause a fluctuation in capacitance. The variation in capacitance achieved in this way is rather small and, therefore, susceptible to external influences, such as heating up the measurement setup. This leads to changes in the bit string and, hence, to unreliable fingerprints. The change in design and measurement setup improved the reliability of the coating PUFs [15]. A further disadvantage of the coating PUFs is the following: Every measured capacitor adds just one bit to the key. For high security standards, the bit string should be at least 128-bits long. For coating PUFs, longer bit strings lead to more capacitors, which must be additionally fabricated on the wafer. This leads to the objective that every capacitor should add several bits to the key.

In this paper, a 2-bit key per capacitor for coating PUFs is presented for the first time. In order to achieve this goal, a larger fluctuation in capacitance is necessary. This is accomplished through the implementation of a self-developed layer made of spin-on glass (SOG) with aluminum particles. In addition, the range in capacitance value will be adjusted using different dielectric materials. In order to prove the randomness of our process, 49 chips per wafer for 3 different wafers were fabricated and analyzed. To the best of our knowledge, capacitor structures for coating PUFs were produced and analyzed on several whole wafers for the first time. The optical and electrical results show that the large variation in capacitance was achieved through different particle sizes and random distribution. In the end, the 1-bit key was compared to the 2-bit key in terms of PUF reliability and quality.

II. THE CAPACITOR STRUCTURE

In capacitive coating PUFs, each capacitor generates one bit for the bit string. In this case, one decision value is selected, usually the capacitance mean value of all measured capacitors. If the measured capacitance is greater than this value, a logical 1 is stored. Should it be lower, a logical 0 is stored [15]. To divide the measured values in 4 sections, three decision values are required for the 2-bit key per capacitor. It becomes important to create a large fluctuation in capacitance. All reported capacitive coating PUFs show a fluctuation that is too low. This circumstance would lead to exceptionally narrow decision values, which result in high error rates and unreliable keys [13], [15].

A. CONCEPT

The classical particle layer of coating PUFs consists of titanium nitride and aluminum oxide particles. They are embedded in a polymer [13]. This causes only a slight fluctuation in capacitance, since the particles only make a small contribution to the total capacitance. The reason for this is that the partial capacitances of the entire capacitor are mostly connected in series. In order to achieve a high fluctuation, the partial capacitances must be parallel to each other. This increases the contribution of the particles to the total capacitor.

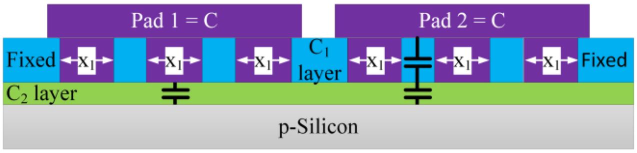


FIGURE 1. Concept of the capacitor model.

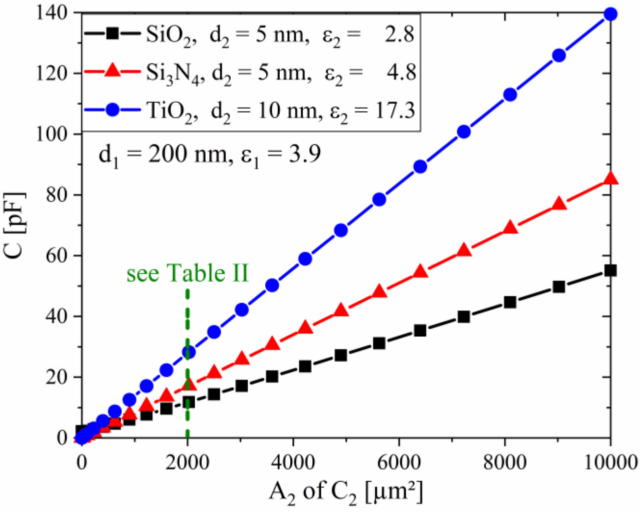


FIGURE 2. Contribution of C_2 with varying area A_2 and dielectric material to the total capacitance C for each PUF pad 100 x 100μm^2. As dielectric material, SiO_2, Si_3N_4, and TiO_2 are used. Capacitance C_1 consists of 200 nm thick SiO_2.

Fig. 1 shows the proposed design for a metal oxide semiconductor (MOS) capacitor. As an introduction, two capacitor pads are shown. They were fabricated in a fixed design without the desired random fluctuations. The concept is based on the fact that there are two different capacitances in our capacitor: a high partial capacitance C_2 and a low partial capacitance C_1. This can be achieved by using two different layers as dielectric material (layer C_1 and layer C_2), which can vary in thickness or dielectric constant.

In this concept, there is one part, wherein C_1 and C_2 are connected in series. This part capacitor C_3 is given in equation 1. In this case, the smaller part capacitor C_1 dominates.

$$C_3 = \frac{C_1 \times C_2}{C_1 + C_2}. \qquad (1)$$

In addition, C_3 is connected parallelly to the partial capacitance C_2, where the aluminum makes direct contact with the C_2 layer. If we assume that the areas of the partial capacitors are identical, we arrive at the following equation:

$$C = n \times C_3 + m \times C_2. \qquad (2)$$

In the case of Fig. 1, the variables m and n are equal to 3. For the overall capacitor C, the partial capacitance C_2 dominates. This means that the higher the amount of m respectively area A_2 is, the higher C will be (Fig. 2). It is also clearly discernible that even a small change in m respectively area A_2 of C_2 leads to a significant change in C. The use of a material with higher dielectric constant for C_2 leads to higher C and even greater fluctuations in capacitance. This should lead to a high variation in total capacitance C, which is required for the 2-bit system.

An important fact for this concept is that the number of C_2 must be completely random and unpredictable. Hence, what is needed is a thick dielectric layer with random holes that can be used in the back-end of line.

B. FABRICATION OF THE CAPACITOR STRUCTURES

The fabrication of the capacitor structures for PUF begins with a p-type (10-20 Ωcm) 100-mm silicon bulk wafer that is cleaned via standard wet cleaning. Thereafter, the dielectric material for the capacitor C_2 is fabricated. Three different materials were used in the context of this work: silicon oxide (SiO_2), silicon nitride (Si_3N_4), and titanium dioxide (TiO_2).

In the case of SiO_2, the process started with a hydrofluoric acid dip (HF) for substrate cleaning. Afterwards, the SiO_2 layer was thermally grown by a rapid thermal process (RTP) at 750 °C for 4 minutes in an oxygen and hydrogen atmosphere. The thickness achieved is approximately 5 nm.

The second material is Si_3N_4. The advantage of this material is that it has a higher dielectric constant than SiO_2. This material was deposited using a low-pressure chemical vapor deposition (LPCVD) process at 740 °C in a dichlorosilane and ammonia atmosphere. A process time of 170 seconds was necessary to achieve a thickness of about 5 nm.

The third material is TiO_2, which has the highest dielectric constant of all three materials used. It was deposited by reactive sputtering at 750 W in an oxygen and argon atmosphere. The process time to achieve a thickness of about 10 nm was 5 minutes. For better electrical properties, the material was annealed with an RTP at 600 °C for 1 minute in an oxygen atmosphere.

The next step was to deposit the dielectric material for C_1. In our case, spin-on glass (SOG), a typical back-end of line material, was used. This liquid solution was spun on a silicon wafer. After baking, a homogenous SiO_2 layer was created. For the presented concept, we needed randomly distributed holes in our layer. In order to achieve holes in the SOG, aluminum particles with a size of 80 μm were added to the solution. The slurry of 25 ml was dispersed with an ultrasonic compressor UP200s at 50-60 Hz for 2 x 30 seconds. This is necessary to avoid quick agglomeration and sedimentation of the slurry. The thusly prepared solution was spun on the wafer for 10 seconds at 3000 rounds per minute (rpm) and baked out at 80 °C, 150 °C, and 250 °C for 1 minute each. Via this process, a SiO_2 layer with more or less randomly distributed aluminum particles was created. This led to random variations in distances a_i and diameter x_i of the particles (Fig. 3a).

Thereafter, the aluminum particles were removed by wet etching. In this case, a phosphorous etching solution (PNA) was used at 40 °C for several hours. After this process, the particles were completely removed and left behind randomly distributed holes in the SOG (C_1 layer).

For the top electrode of the capacitor, aluminum was evaporated. This was necessary, since a sputter process could cause plasma damages to the thin dielectric material used for C_2. The top electrode was patterned by optical lithography and wet chemical etching (Fig. 3b). After the backside oxide was removed by an HF-dip, the bottom electrode of the capacitor was fabricated by evaporation of aluminum.

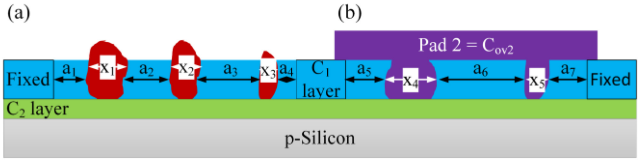


FIGURE 3. Cross-section of the fabricated capacitor, (a) after deposition of the particle SOG, (b) after removing the particles and patterning of the MOS capacitor pads.

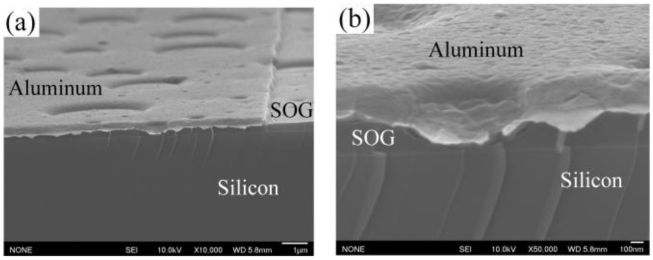

(a)
Aluminum
SOG
Silicon
NONE SEI 10.0kV X10,000 WD 5.8mm 1μm
(b)
Aluminum
SOG
Silicon
NONE SEI 10.0kV X50,000 WD 5.8mm 100nm

FIGURE 4. SEM images of the fabricated MOS capacitors, (a) overview of an aluminum pad with various holes, (b) zoomed view on a hole created by a particle.

With this process sequence, 49 identical PUF chips, which are used for electrical measurements, were fabricated. Each PUF chip consisted of 195 MOS capacitors with a size of 100 x 100 μm^2. It should be mentioned that the whole PUF structure can be deposited at any underlying chip structure. This allows universal use.

C. OPTICAL EVALUATION OF THE PARTICLE LAYER

For evaluation of the particle layer, MOS capacitors were fabricated using SiO_2 as dielectric material for C_2. Fig. 4 shows scanning electron microscope (SEM) images of the thusly manufactured MOS capacitors. One can clearly discern that the particles created holes in the SOG. Due to the usage of the ultrasonic compressor, the size of the particles and holes varied.

In Fig. 4a, all particles were removed during etching. The created holes differed in size and were randomly distributed. Through the evaporation process, the holes were covered conformally by aluminum (Fig. 4b). In the hole, the thickness of the SiO_2 was just 5 nm. Around the hole, however, the thickness of 200 nm was given by the SOG. This proves that the capacitance of the whole pad will now vary because of the different areas of dielectric materials. In addition, it's visible that the area in which the aluminum touches the thin SiO_2 is smaller than expected in the top view.

Additional observations of the particle layer were made by using a microscope and a 3D microscope by Keyence. The top view of the MOS capacitors is shown in Fig. 5a. The holes turned out to be much larger than the used particles.

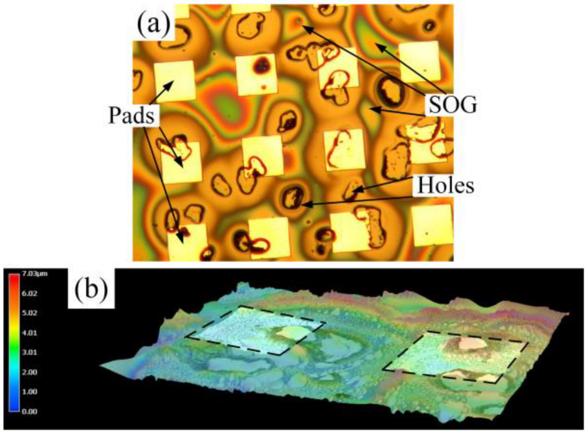


FIGURE 5. Microscope images of the MOS capacitors, (a) top view, (b) detailed view on surface roughness (dashed box represents the capacitor pad).

This is due to the fact that the particles tend to cluster. If the density of particles is too high, the SOG starts to tear. As a result, it's possible that the entire aluminum pad is located on the thin SiO_2. It could be observed that this effect is random and varies from capacitor to capacitor.

In Fig. 5a, interference patterns could be observed in the SOG. From this, it was possible to conclude that the SOG was no longer homogenous but varied in thickness. This would cause an additional variation in capacitance. This inhomogeneity has been confirmed through a 3D microscope image (Fig. 5b). It should be emphasized that the change in capacitance through the inhomogeneity of the SOG will be much smaller than through the different dielectric materials.

The optical evaluation proved that the particle layer caused a random change in the dielectric material of the capacitors. The fluctuation in capacitance depends on the following:

- number of holes,
- size of the hole,
- tearing of the SOG,
- inhomogeneity of the SOG.

III. MEASUREMENT RESULTS

In [15], we presented an electrical measurement setup to reliably measure the fluctuation in PUF MOS capacitors that has been introduced through processing. Hence, we used the 4980A LCR-Meter from Keysight and, to measure all chips on the wafer, a semiautomatic prober from Cascade. From the thusly achieved CV curves, the highest capacitance value in accumulation is read out. This value was then used to generate the PUF key. The measurement setup has a capacitance accuracy of 0.01 pF.

A. ELECTRICAL MEASUREMENTS OF SINGLE CAPACITORS

The MOS capacitors were fabricated with the above-mentioned method. SiO_2 with a thickness of 5 nm and SOG with particles were used as dielectric materials. Fig. 6 shows the CV curve of various capacitors measured on one single chip. The fluctuation of the capacitance in accumulation is clearly visible. The larger the holes through the particles or the greater their number is, the higher the capacitance will be. If no holes can be found in the capacitor, the capacitance in accumulation will be determined by the SOG and, therefore, be very small. Due to the inhomogeneous SOG, which was already shown by the optical inspection, a variation in capacitance was observed for capacitors without holes. This fluctuation turned out to be exceptionally small because the variation in SOG thickness was very slight.

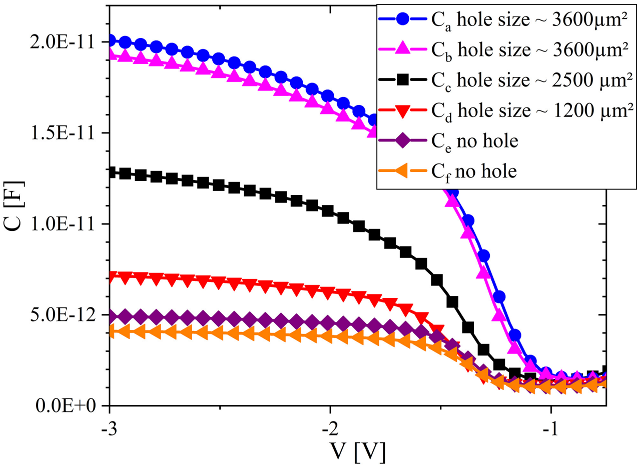


FIGURE 6. CV curves of various MOS capacitors with different hole sizes.

TABLE 1. Minimum and maximum values of measured capacitances in accumulation.

Material	Particle-free SOG, C_1 (min)	Without SOG, C_2 (max)
SiO_2	2.8 pF	48 pF
Si_3N_4	2.2 pF	85 pF
TiO_2	1.5 pF	140 pF

Comparing the theory in Fig. 2 with the obtained results of Fig. 6, C_a has a hole size of approximately 3600 μm^2, C_c of approximately 2500 μm^2, and C_d of approximately 1200 μm^2. This shows that a small change in hole area makes a large difference in capacitance.

To determine the maximum range of capacitance values for C_1 and C_2, capacitors were fabricated using different C_2 layers with particle-free SOG and without SOG. The capacitance values for C_2 are always much larger than for C_1 (Table 1). They are negligible if both capacitors are connected in series. This observation proves that we have a serial circuit between C_1 and C_2. The largest range in capacitance can be observed for TiO_2, which has the highest dielectric constant.

B. ELECTRICAL MEASUREMENTS FOR THE WHOLE CHIP

In this part, a whole chip with 195 capacitors was measured and analyzed. They were arranged in a matrix consisting of 15 rows and 13 columns.

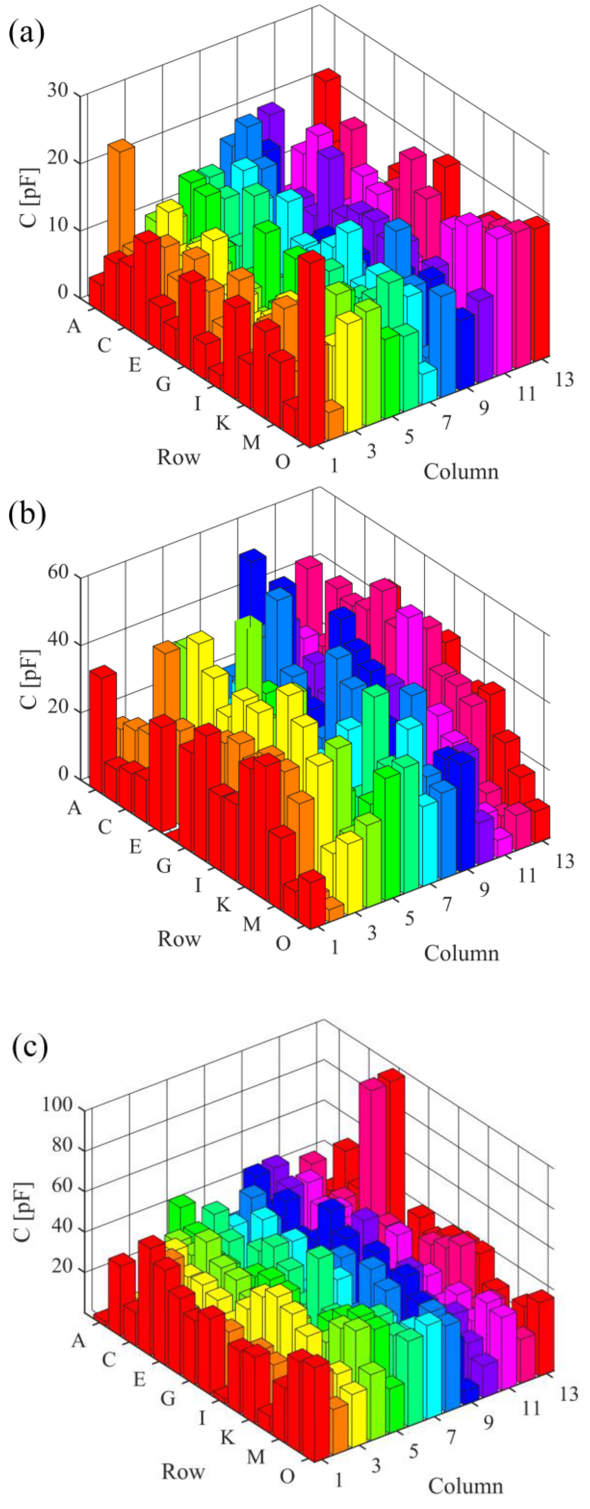


FIGURE 7. 3D plot of exemplary chips with 195 capacitors but different dielectric materials, (a) SiO_2, (b) Si_3N_4, (c) TiO_2 for C_2.

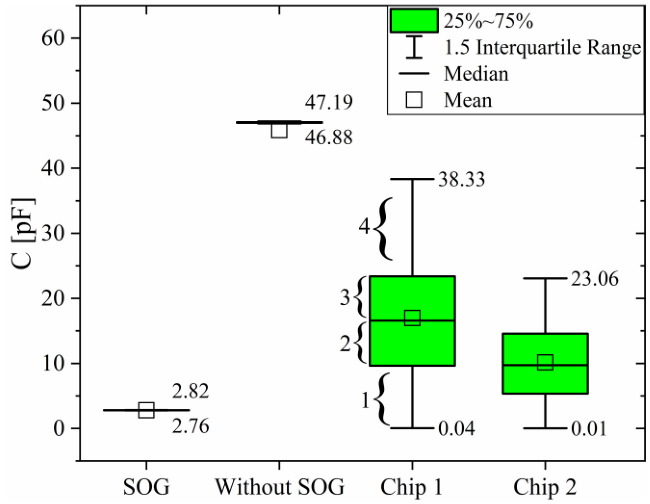


FIGURE 8. Box-and-whisker plot for SiO_2 as dielectric material for C_2 and fabricated capacitors without SOG, with particle-free SOG and particle SOG (Chip 1, Chip 2). For Chip 1, the sections for the 2-bit key are shown exemplarily.

In Fig. 7, we see exemplary chips with 195 capacitors, where each bar represents one capacitor. The chips differ in the use of different dielectric materials. For a chip fabricated with SiO_2, the capacitances fluctuated from 3 pF to 36 pF. An exemplary chip is shown in Fig. 7a, which does not represent the full range possible in order to highlight the variations between the various PUF structures.

Although the capacitors are closely together, the capacitances can change significantly from one capacitor to the other. These findings are comparable to the results obtained using Si_3N_4 or TiO_2 as dielectric layer (Fig. 7b and 7c). For Si_3N_4, the capacitances fluctuated from 4 pF to 62 pF. Through the usage of TiO_2, the fluctuation was shifted to even higher values, 2 pF to 98 pF. The variation of the capacitors can be adjusted by using different dielectric materials for the C_2 layer.

These obtained results are comparable with the theory in Fig. 2. They are the largest published capacitance fluctuations for coating PUFs to date [13], [15]. This shows that the process can be used for different dielectric materials, without damaging the MOS capacitors.

In order to prove that the obtained fluctuation depends on our particle SOG, various capacitors were fabricated. In this case, we used SiO_2 as dielectric material for C_2 and fabricated capacitor chips with SOG, without SOG and with particle SOG.

The obtained results are displayed in the box-and-whisker plot in Fig. 8. For every fabricated wafer, an exemplary chip is shown. The range in capacitance for the chips fabricated without and with particle-free SOG is very small. This proves that the RTP (SiO_2) and the particle-free SOG deliver homogenous layers. In this case, small measurement changes, like heating up of the equipment, could lead to a change in capacitance. Although the properties of the C_1 and C_2 layer are very reliable, this makes it difficult to generate a reliable PUF key, even more if the goal is to obtain 2-bit per capacitor key. In order to obtain the necessary fluctuation in capacitance by inhomogeneity of the layers, our developed SOG particle layer must be used. The range in capacitances is so expanded that possible measurement inaccuracies are negligible.

In Fig. 8, the two presented chips differ in mean value and capacitance range. This proves that the capacitances vary from chip to chip. The same results were obtained using Si_3N_4 and TiO_2.

C. ELECTRICAL MEASUREMENTS FOR 49 CHIPS

The last chapter proved that the capacitance of the capacitors varies within a chip. To determine if the capacitances vary from chip to chip, 49 chips with 195 capacitors were measured.

Another important aspect is how the particles are distributed on the wafer. In terms of realizable security issues in the application, a change in distribution from wafer to wafer would be favorable. This would make the process even more unpredictable and unclonable. To the best of our knowledge, this observation has not yet been published for multiple chips on different wafers.

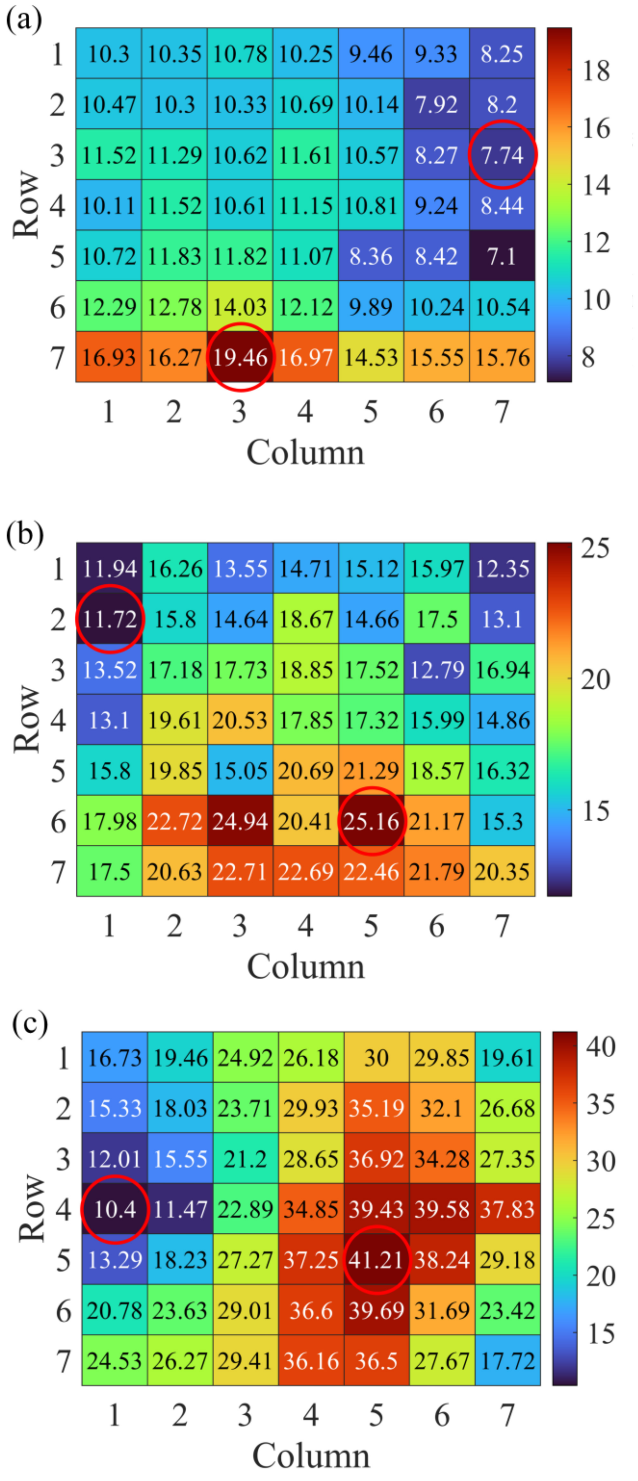
In Fig. 9, heat plots are shown for three wafers, with particle SOG on different dielectric materials for C_2. The measured chips are arranged according to their position on the wafer in a 7x7 matrix. For each chip, the mean value of the 195 capacitors is illustrated.

All three wafers show that there are certain chips with high mean values (red) and some with low values (blue). This depends on the number of created holes, which have been found on a particular chip. The position of the chips with high mean values varies from wafer to wafer. The same observation can be made for chips with low mean values. This proves that the distribution of the particles is random on the chip, from chip to chip, and from wafer to wafer. Each wafer has its characteristic distribution of particles on every chip. These distributions are formed in the spin coating process with 3000 rounds per minute (rpm). The particles are distributed randomly over the entire wafer and there is a difference from wafer to wafer as to where the highest particle density occurs.

Furthermore, it's possible to observe that the chips with high or low mean values can be next to each other, which supports the fact that the particle distribution is really random. Please be aware that normally, the consumer does not exactly know which position their chip has on the wafer. Hence, the clustering of particles at chips nearby is not a big issue.

Fig. 10 shows the distribution of all 9555 capacitance values of 49 chips per wafer for three wafers with different C_2 layers. The distribution varies for each wafer and shows that there is a wide range of capacitance values above and below the distribution maximum achieved. This confirms that the particles and the resulting holes cause a large variation in capacitance across the 49 chips. None of the displayed distributions is normally distributed.

A visible difference is observed for the different dielectric materials. The higher the dielectric constant of the layer, the more the distribution shifts to higher capacitance values, and the more the effect of each created hole is emphasized. This is visible in the two peaks at 2 pF and 35 pF for the distribution of TiO_2, where every small particle has a large effect on the total capacitance. For the other two materials, this cannot be observed, because the dielectric constant is too small and the distribution of the holes is different.



(a)

Row	1	2	3	4	5	6	7
1	10.3	10.35	10.78	10.25	9.46	9.33	8.25
2	10.47	10.3	10.33	10.69	10.14	7.92	8.2
3	11.52	11.29	10.62	11.61	10.57	8.27	7.74
4	10.11	11.52	10.61	11.15	10.81	9.24	8.44
5	10.72	11.83	11.82	11.07	8.36	8.42	7.1
6	12.29	12.78	14.03	12.12	9.89	10.24	10.54
7	16.93	16.27	19.46	16.97	14.53	15.55	15.76

(b)

Row	1	2	3	4	5	6	7
1	11.94	16.26	13.55	14.71	15.12	15.97	12.35
2	11.72	15.8	14.64	18.67	14.66	17.5	13.1
3	13.52	17.18	17.73	18.85	17.52	12.79	16.94
4	13.1	19.61	20.53	17.85	17.32	15.99	14.86
5	15.8	19.85	15.05	20.69	21.29	18.57	16.32
6	17.98	22.72	24.94	20.41	25.16	21.17	15.3
7	17.5	20.63	22.71	22.69	22.46	21.79	20.35

(c)

Row	1	2	3	4	5	6	7
1	16.73	19.46	24.92	26.18	30	29.85	19.61
2	15.33	18.03	23.71	29.93	35.19	32.1	26.68
3	12.01	15.55	21.2	28.65	36.92	34.28	27.35
4	10.4	11.47	22.89	34.85	39.43	39.58	37.83
5	13.29	18.23	27.27	37.25	41.21	38.24	29.18
6	20.78	23.63	29.01	36.6	39.69	31.69	23.42
7	24.53	26.27	29.41	36.16	36.5	27.67	17.72

FIGURE 9. Heat plots with mean value per chip of 3 different wafers, with 49 chips and particle SOG on different dielectric materials, (a) SiO_2, (b) Si_3N_4, (c) TiO_2 for C_2.

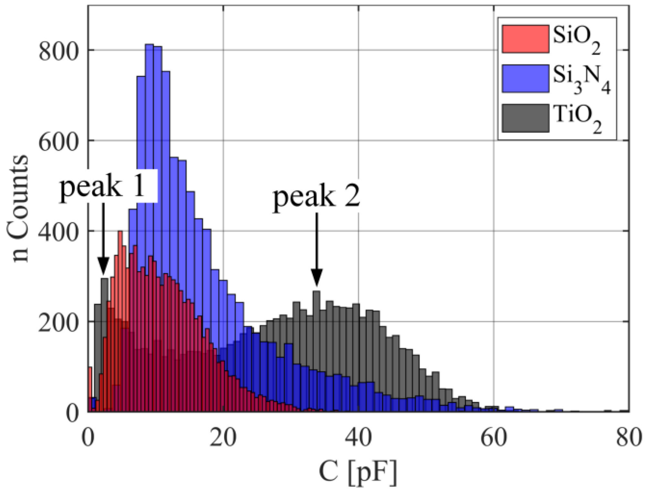


FIGURE 10. Distribution of all capacitance values of 49 chips per wafer, depending on the dielectric material for C_2.

TABLE 2. Mean value of capacitance per wafer.

Material	Mean value	Standard deviation
SiO_2	11.16 pF	± 11.24 pF
Si_3N_4	17.61 pF	± 6.30 pF
TiO_2	27.10 pF	± 15.04 pF

In Table 2, the mean values for all of the three wafers are given. The highest total mean value was achieved for TiO_2, because it delivers the highest dielectric constant. Comparing these values with the theory given in Fig. 2, the average hole size can be determined. The values from Table 2 all lie on a straight line and intersect the x-axis at 2000 μm^2 (see dashed line in Fig. 2). This is the average area of the partial capacitance C_2. The circumstance that all mean values lie on a straight line proves that the same number of particles per SOG was spun on the whole wafer. This demonstrates that the change in local distribution in Fig. 10 is just given by the random distribution of the particles on the wafer, the difference in particle size, and the different dielectric materials.

IV. PUF KEY GENERATION AND EVALUATION

A key must be generated to use the created chips as PUF structures. This section describes two different concepts to generate the PUF key: 1-bit per capacitor key and a 2-bit per capacitor key. Later, the thusly gained bit strings shall be compared, the quality of the PUFs determined.

A. 1-BIT PER CAPACITOR KEY

In the case of a 1-bit per capacitor key, every capacitor generates 1-bit. As decision value, the median value of all measured 9555 capacitors on a wafer is chosen. If the measured capacitance value of each PUF capacitor on each chip is higher than the decision value, a logical 1 is stored. A logical 0 is stored if the value is lower than the decision value. In Fig. 11, such a PUF code is shown for two different chips on the same wafer. In this case, green represents a logical 1 and gray a logical 0. The length of the bit string is 195, since this is the number of capacitors on one chip. The mean value of 1 and 0 is around 50% in both cases, which corresponds to the theoretical ideal value [16].

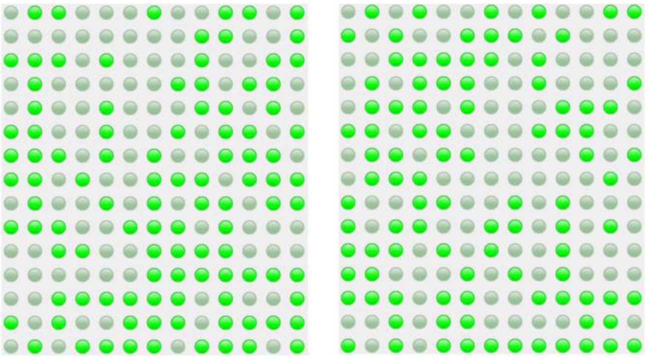


FIGURE 11. 195-bit PUF key for two exemplary chips fabricated with SiO_2 as dielectric material on one wafer. The first chip on the left has 52.8% logical 1 (green) and 47.2% logical 0 (gray). The second chip on the right has 49.7% logical 1 and 50.3% logical 0.

B. 2-BIT PER CAPACITOR KEY

The 2-bit per capacitor key has the advantage that every capacitor represents two bits. This means that every capacitor may possess 4 different values: "00", "01", "10", "11". Other groups that show 2-bit systems only have 3 different values [18], [19]. To determine the 2-bit key, 3 decision values are needed. In this case, the 9555 measured capacitance values on one wafer are sorted in an ascending order. The first decision value is the capacitance value, which is on place number 2389 (p1), the second on 4778 (p2), and third on 7167 (p3). Depending on the capacitance value C for each PUF capacitor, the following bit code is generated:

$$\begin{aligned} c < p1 &=> 00\\ p1 < c < p2 &=> 01\\ p2 < c < p3 &=> 10\\ c > p3 &=> 11. \end{aligned} \tag{3}$$

In Fig. 12, the 2-bit per capacitor key is shown for the same two chips as in Fig. 11. The length of the bit string is now doubled from 195 to 390. The mean value of 1 and 0 is, in both cases, around 48%, which is close to the ideal value of 50%. In this case, using the 2-bit per capacitor key leads to the generation of slightly more 0 than 1.

C. EVALUATION AND COMPARISON OF THE PUFS

For evaluation and quality of PUFs, various criteria have been published [16], [17]. All of these criteria attempt to describe the uniformity, uniqueness, and reliability of the structure.

The Hamming weight (HW), which is also referred to as the mean value, describes the randomness of the response of one single PUF chip [16], [17]. The HW is described with

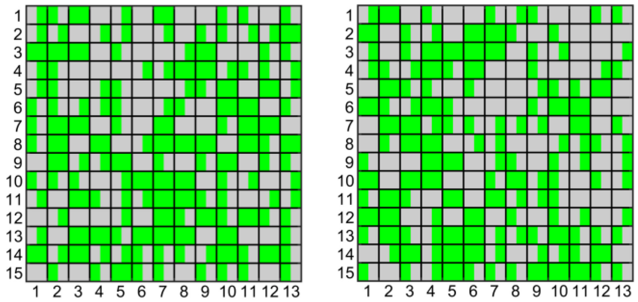


FIGURE 12. 390-bit PUF key for two exemplary chips fabricated with SiO_2 as dielectric material on one wafer; color code within one PUF capacitor (black box) ,00 (gray gray), 01 (gray green), 10 (green gray), 11 (green green). The first chip on the left has now 48.9% logical 1 (green) and 51.1% logical 0 (gray). The second chip on the right has 46.4% logical 1 and 53.6% logical 0.

TABLE 3. Mean value (μ) and standard deviation (σ) of the histograms of the fabricated PUFs for entire wafers.

		SiO_2		Si_3N_4		TiO_2	
		μ	σ	μ	σ	μ	σ
ACF	1-bit	0.003	0.09	0.003	0.09	0.003	0.09
	2-bit	0.001	0.06	0.001	0.07	0.001	0.07
HW [%]	1-bit	50.02	14.70	50.01	14.96	49.99	25.61
	2-bit	50.02	11.91	49.99	11.19	50.00	18.53
HD_{inter} [%]	1-bit	48.68	4.64	48.55	4.03	49.98	3.61
	2-bit	48.94	3.70	49.03	2.55	50.02	2.11
BA [%]	1-bit	50.02	7.13	50.01	7.42	49.99	6.09
	2-bit	50.02	7.33	49.99	7.42	50.00	6.58

following equation:

$$\mathrm{HW} = \left(\frac{1}{\mathrm{N}}\sum_{\mathrm{i}=1}^{\mathrm{N}} \mathrm{r_i}\right) \times 100\%. \tag{4}$$

N describes the number of bits of a chip, with r_i being the actual output of the bit. To get the highest possible unpredictable output of the PUF, the number of logical 0 and 1 must be evenly distributed on the PUF chip. For this reason, the optimum value of the HW is 50%. If the value deviates significantly from the ideal value of 50%, the response of the PUF chip is biased either to more logical 1 or more logical 0. In this case, an attacker can solve the code faster by guessing that the response is biased to a certain value. It depends solely on the application to determine which values of HW are still acceptable [16]. In practice, fuzzy extractor and error corrections are used to minimize the biased output [20].

Figure 13a shows the HW of all 49 chips on three wafers using the 1-bit key. For the chips using SiO_2 for C_2, the distribution of the single chip HW has a maximum at the ideal value of 50%. For Si_3N_4 and TiO_2, the maximum in the HW distribution is not at 50%. Due to the choice of the median value of all measured capacitors on a wafer as the decision value, the HW mean value for all 49 chips per wafer is 50% (Table 3). The higher the dielectric constant of the dielectric material, the more disperse are the values of the HW. This is confirmed by the standard deviation values (Table 3). The values displayed are well above the ideal value of 6.98% ($\sigma = \sqrt{195}/2$). The reason for this is provided in Fig. 9. It can be seen in the figure that the mean value of the capacitances per chip varies a great deal for all dielectric materials, but especially for Si_3N_4 and TiO_2. This means that some chips have plenty of small capacitance values or especially high capacitance values. Taking the median of all measured capacitors as the decision value will result in some chips having more logical 0 or logical 1. The results obtained on the dielectric materials with a high dielectric constant such as Si_3N_4 and TiO_2 highlight this effect. This problem can be avoided for the 1-bit key by using a different decision value such as the median value of every single chip. In the work presented, the median value of all measured capacitors on a wafer were examined in order to be able to better compare the 1-bit key with the 2-bit key. Taking the median of each individual chip would result in an incorrect comparison.

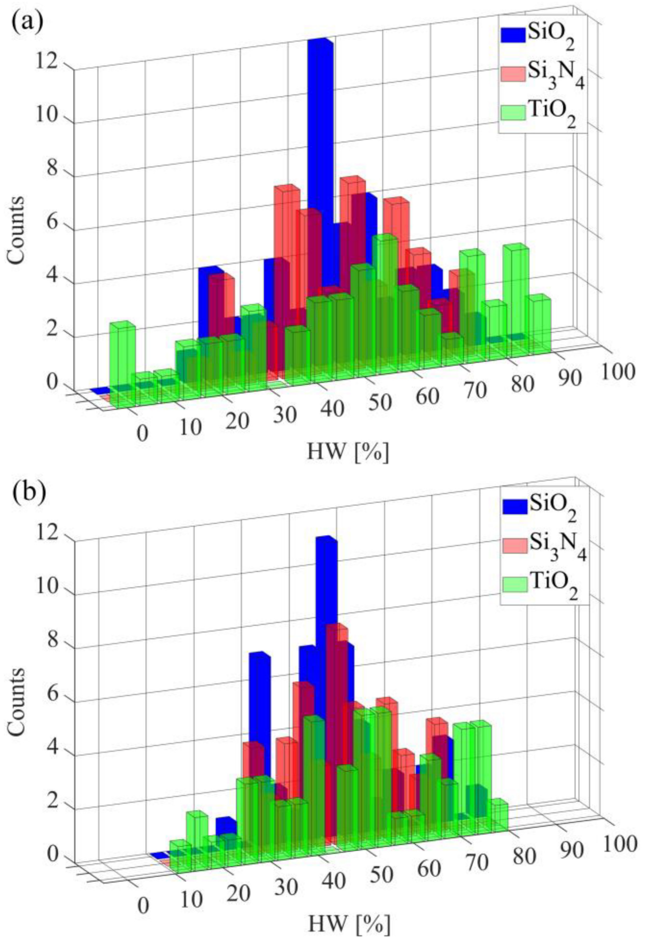


FIGURE 13. Hamming weight of all 49 chips on 3 wafers (a) 1-bit key, (b) 2-bit key.

The HW for all 49 chips on three wafers using the 2-bit key shows a similar result compared to the 1-bit key (Fig. 13b). As previously observed, the HW mean value for all 49 chips per wafer is 50% (Table 3). For all wafers the fluctuation of the HW is significantly suppressed. This is confirmed by the standard deviation values, which are now much smaller compared to the 1-bit key (Table 3). The values are also significantly closer to the ideal value of 9.88% ($\sigma = \sqrt{390}/2$). By using the 2-bit key, chips that tended to have a high number of logical 0 or logical 1 are now more balanced. This occurs because capacitors with a logical 0 as the first bit tend to generate a logical 1 as the second bit. Capacitors with logical 1 as the first bit tend to generate a logical 0 as the second bit. This case applies to 50.1% of the capacitors on one whole wafer, for this reason the negative correlation between the first bit and the second bit is negligible. Moreover, this is confirmed by the analysis of the autocorrelation function.

Due to the large fluctuation in HW, the 1-bit key seems to be not very useful for TiO_2 capacitors. An attacker could guess the outcome of certain PUF chips, since they are extremely biased. In this case, a high effort on error correction would be necessary.

Another aspect to consider, when looking at individual PUF chips, is whether neighboring bits influence each other. Such a correlation between bits would allow an attacker to predict the result. The autocorrelation function (ACF) is used to determine whether there is a correlation between bits in the PUF chip [16], [21], [22].

$$R_{xx}(j) = \sum_{n} x_n x_{n-j} \tag{5}$$

R_{xx} is the correlation between bits for a distance lag j. If R_{xx} is equal to 1 or −1, the bits are fully correlating at lag j. The bits are completely uncorrelated when the ACF is 0. With the structure presented here, there can be a correlation between bits if neighboring bits influence one another due to layout, particle clustering or a lack of particles.

Fig. 14 shows the autocorrelation of a typical chip with SiO_2 as the dielectric material for C_2. At lag 0 the correlation is equal to 1, because each bit is fully corelated with itself. A clear pattern for the chips, which would indicate a layout problem, is not visible.

In Fig. 14a, the autocorrelation for a prototypical chip for the 1-bit key shows a very low value of 0.003, which is close to the ideal value of 0. This indicates that there is no correlation between bits. Some points lie at approximately 0.14, which suggests a slight correlation. This may be because some particles can cause large cracks in the SOG, which means that neighboring capacitors tend to have a high capacitance. This results in many neighboring capacitors having a logical 1 and therefore slight correlation in bits. This can also happen when neighboring capacitors have a logical 0 because large particles are missing. Table 3 shows the mean value and standard deviation for the autocorrelation for all 49 chips on a wafer. All chips show the same autocorrelation values regardless of the dielectric material used for C_2. The standard deviation also indicates that only occasionally some bits are negligibly correlated.

Fig. 14b shows the autocorrelation for the same prototypical chip but instead when using the 2-bit key. In this case, the autocorrelation improves from the 1-bit key to a value of 0.001. This shows that there is no correlation between bits. Table 3 displays that all chips have the same mean autocorrelation and standard deviation values, regardless of the dielectric material used for C_2. This shows that using the 2-bit key suppresses the correlation between bits caused by cracking in the SOG or smaller sized particles.

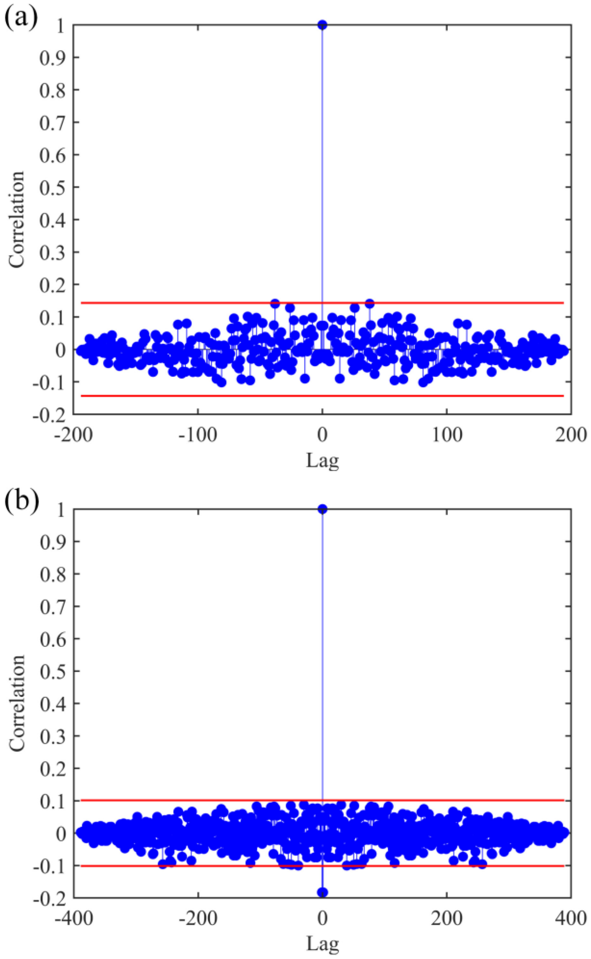


FIGURE 14. Autocorrelation of one typical chip with SiO_2 as the dielectric material on one wafer, (a) 1-bit key, (b) 2-bit key. The red lines indicate the 95% confidence level.

Nevertheless, the autocorrelation values for both the 1-bit key and the 2-bit key are very good and have not yet been shown by others for coating PUFs. The results obtained are similar to those of SRAM-PUFs [21], [22].

Due to security issues, it is important to know if the PUF chips correlate with each other. This would mean that certain bits, in our case capacitors, would tend toward a certain value. Should this be the case, then knowing the output of one chip would make it easier to determine the output of the next chip. This would lead to a low chip security.

To determine if the PUF chips do not correlate and are unique, the inter-chip Hamming distance (HD_{inter}) is introduced. The HD_{inter} for two chips u, v with the outputs r_u, r_v for a group of m chips is described using the following

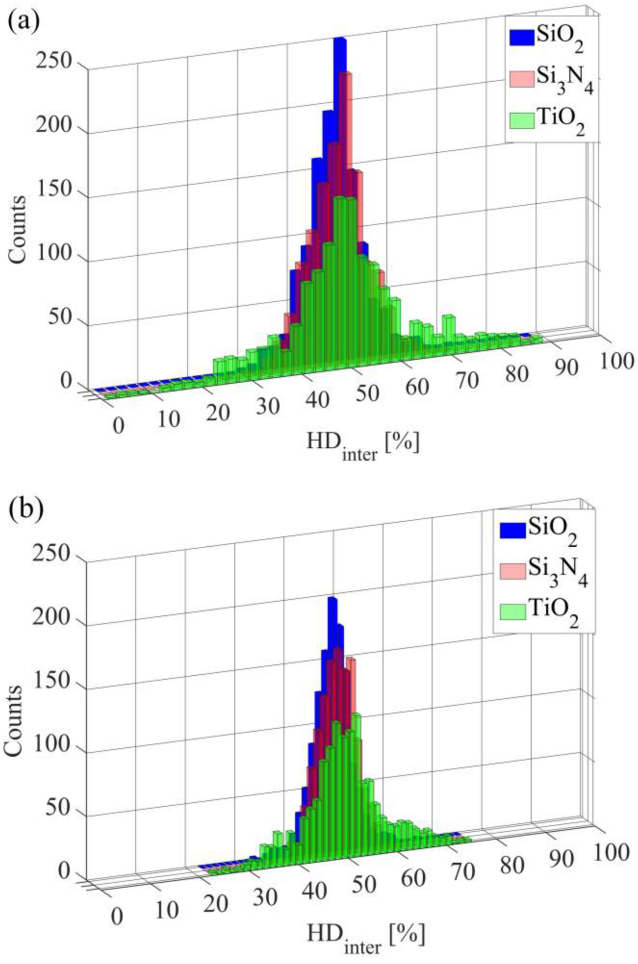


FIGURE 15. Inter-chip Hamming distance for all 49 chips on 3 wafers, (a) 1-bit key, (b) 2-bit key.

expression:

$$\mathrm{HD_{inter}} = \frac{2}{\mathrm{m(m-1)}} \sum_{\mathrm{u=1}}^{\mathrm{m-1}} \sum_{\mathrm{v=u+1}}^{\mathrm{m}} \frac{\mathrm{HD(r_u, r_v)}}{\mathrm{N}} \times 100\%. \quad (6)$$

A $\mathrm{HD_{inter}}$ value of 0% or 100% would mean that no or all bits are changing and, therefore, the output can be predicted. These results would lead to less security, because an attacker could easily predict the response. To achieve a maximum of unpredictability, the value of the $\mathrm{HD_{inter}}$ must be at 50%.

In Fig. 15, the $\mathrm{HD_{inter}}$ of 49 chips on the three fabricated wafers is displayed. For the 1-bit key, the values, as predicted by the theory, are distributed normally (Fig. 15a) [16]. The histogram shows that the $\mathrm{HD_{inter}}$ for the wafers using $\mathrm{SiO_2}$ and $\mathrm{Si_3N_4}$ fluctuate slightly and have a maximum at 50%. For $\mathrm{TiO_2}$, the values for $\mathrm{HD_{inter}}$ disperse comparably to the values of HW.

The histogram for $\mathrm{HD_{inter}}$ using the 2-bit key is only normally distributed for $\mathrm{SiO_2}$ (Fig. 15b). In this case, for all three wafers, we reach a maximum of the $\mathrm{HD_{inter}}$ at 50%. When using the 2-bit key, the fluctuation of the values is even suppressed for $\mathrm{TiO_2}$.

Table 3 shows the mean and standard deviation values for $\mathrm{HD_{inter}}$ for the entire wafer with 49 chips. It indicates that the mean value for the 1-bit key is slightly below the ideal 50% but for the 2-bit key it approaches 50%. These results indicate that the PUF chips do not correlate with one another for either the 1-bit key or the 2-bit key. The obtained values for the standard deviation are in an acceptable range, but are improved by using the 2-bit key. This is because the HW fluctuates less with the 2-bit key, so $\mathrm{HD_{inter}}$ does the same.

$\mathrm{HD_{inter}}$ detects the correlation between chips. However, a possible correlation between bits is neglected. The information is missing if certain capacitors always deliver the same output bit. This can happen if there is a design error, or if holes are always on the same spot on the chip. To detect this correlation between bits, a bit aliasing (BA) factor is used [17]. It is defined as:

$$\mathrm{BA} = \left(\frac{1}{\mathrm{m}} \sum_{\mathrm{t=1}}^{\mathrm{m}} r_{t,i} \right) \times 100\%. \quad (7)$$

Here, m is the number of chips and $\mathrm{r_{t,i}}$ the response of the bit i for chip t. The ideal value for BA is 50%. If the value for BA is 0% or 100%, the bit tends to be always a logical 0 or a logical 1. In this case, an attacker could always guess the outcome of a certain bit and, because of this, the PUF key could be decoded more quickly.

Fig. 16a shows the BA for the 1-bit key. There is no apparent difference between the various dielectric materials. The range in fluctuation is comparable. The distribution maximum is at the desired 50%. In Table 3 the mean value for the BA for the entire wafer is presented. It is, for all materials, at 50%. A difference in BA between 1- and 2-bit key is not visible (Fig. 16). For the 2-bit key, the distribution looks very similar to the one of the 1-bit key. The overall mean value for the BA is also, in the case of the 2-bit key, around 50% for all materials. This reveals that there is no correlation of the bits, for either the 1-bit or 2-bit key (Table 3). The values for the standard deviation are in an acceptable range and do not show any major differences between the wafers or the bit keys. These results are not surprising since, as already mentioned, the particles are distributed completely randomly on the wafer, respectively chips. This helps to avoid the case that a capacitor always delivers a logical 0 or 1 for all 49 chips at the same point. The distribution of the particles is so random that even with the 2-bit key system a correlation of the bits cannot be determined.

Another factor to determine the quality of a PUF is the error rate, which represents the reliability of the PUF. In the ideal case, the bit string of a PUF should not change, even if the structure is challenged a billion times. The error rate for a chip is given by the intra-chip HD ($\mathrm{HD_{intra}}$), where the HD is determined between a reference bit string ($\mathrm{r_t}$) and the actual bit string ($\mathrm{r'_{t,y}}$) for x measurements [16], [17].

$$\mathrm{HD}_{intra} = \frac{1}{x} \sum_{\mathrm{y=1}}^{x} \frac{HD\left(r_t,\ r'_{t,y}\right)}{N} \times 100\%. \quad (8)$$

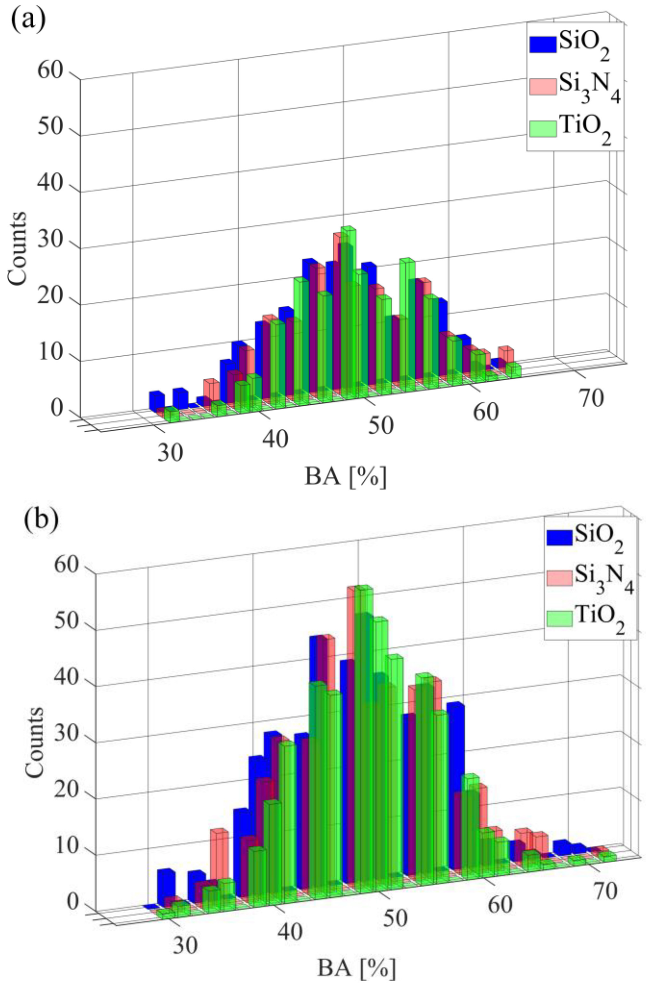


FIGURE 16. Bit aliasing for all 195 bits for 49 chips on 3 wafers, (a) 1-bit key, (b) 2-bit key.

TABLE 4. Comparison of the error rate for one chip at 25°C.

		SiO_2	Si_3N_4	TiO_2
$\mathrm{HD}_{\mathrm{intra}}$	1-bit	0.00 %	0.98 %	0.41 %
	2-bit	0.21 %	2.20 %	1.51 %

In Table 4, the $\mathrm{HD}_{\mathrm{intra}}$ for one chip is given for different dielectric materials. For the measured PUF structure with SiO_2, the error rate for the 1-bit key turned out to be 0% after it was measured 200 times. This is the lowest value which has been published so far for a coating PUF [13], [15]. In comparison, SRAM PUFs show an error rate of 5.47% [23]. For the other two dielectric materials, the obtained error rate was higher than for SiO_2. The reason for this is that some bits are closer to the decision value and because of the accuracy of the measurement setup, which is 0.01 pF, the bits change at certain measurements. Regardless of this situation, by introducing the particle SOG, the error rates were significantly lower than obtained in the previous work when this layer was not used [15].

For the 2-bit key, the error rate worsened for all chips but was comparable to our previous work [15]. The effect of the capacitance values being close to the decision values was amplified. In any case, this demonstrates that the particle layer produces reliable PUF structures. An improvement in the generation of the decision values creates the option to achieve lower error rates.

TABLE 5. Comparison of different PUFs.

PUF types	$\mathrm{HD}_{\mathrm{inter}}$ [%]	$\mathrm{HD}_{\mathrm{intra}}$ (T=25°C) [%]
SRAM [23]	49.72	5.47
Arbiter [23]	49.74	5.89
Ring oscillator [23]	49.60	1.53
This work 1-bit key (TiO_2)	49.98	0.41
This work 2-bit key (TiO_2)	50.02	1.51

The last section showed the results of the analysis of capacitor structures for a PUF with different dielectric materials for C_2. In principle, all three materials are suitable for a PUF chip. The biggest difference between the materials for the 1-bit key can be seen in $\mathrm{HD}_{\mathrm{intra}}$ and $\mathrm{HD}_{\mathrm{inter}}$. On a closer inspection of these two parameters, it appears that SiO_2 would be the material of choice. It has the lowest error rate and acceptable values for $\mathrm{HD}_{\mathrm{inter}}$. TiO_2, on the other hand, has the best values for the 2-bit key. Although its measurement produces a slightly higher error rate than SiO_2. However, in all other parameters it delivers better values and is therefore the material of choice for the 2-bit key.

A comparison with common SRAM, arbiter and ring oscillator PUFs is shown in Table 5. The values for $\mathrm{HD}_{\mathrm{inter}}$ of the capacitive structures presented are comparable with these common PUFs using functional blocks. The capacitor structures with TiO_2 as the dielectric material for C_2 are even more unique than the compared PUFs, regardless of whether we use the 1-bit key or the 2-bit key. A comparison of $\mathrm{HD}_{\mathrm{intra}}$ shows that the chips presented in this work are more reliable at room temperature then state-of the art PUFs. It can therefore be seen that using this capacitive structure as a PUF, regardless of whether the 1-bit key or the 2-bit key is used, can lead to advantages in terms of reliability and uniqueness.

Further investigations should be carried out on the capacitor structures used in this work. The error rate or $\mathrm{HD}_{\mathrm{intra}}$ should be determined for different temperatures and voltages. This is necessary in order to diagnose the stability of these capacitor structures.

V. CONCLUSION

In this paper a 2-bit key per capacitor for PUFs was presented for the first time. This was made possible by developing a particle SOG layer. The results showed that through the particles in the layer, a large fluctuation in capacitance is possible. This fluctuation is completely random, because the size and the distribution of the particles vary from chip to chip and from wafer to wafer. The range of the capacitance value was adjusted by using different dielectric materials. Due to these large fluctuations, a 2-bit key per capacitor could be realized. The evaluation of the PUFs shows that the 2-bit key is as unique and reliable as the 1-bit key for all three dielectric materials. For very large ranges of capacitance, the 2-bit key is more unique than the 1-bit key. Further work should concentrate on the ageing and temperature dependence of the chips – although a change from MOS to metal-dielectric-metal capacitors, which can be used as a final cover layer on basically all underlying devices, opens the possibilities for new applications. In addition, a readout circuit should be designed on the underlying chip in order to generate the PUF key on the chip.

REFERENCES

[1] Ch. Böhm and M. Hofer, "Introduction chapter 1," in *Physical Unclonable Functions in Theory and Practice*, 1st ed. New York, NY, USA: Springer, 2013, pp. 3–38.

[2] D. E. Holcomb, W. P. Burleson, and K. Fu, "Initial SRAM state as a fingerprint and source of true random numbers for RFID tags," in *Proc. Conf. RFID Security*, vol. 7, 2007, pp. 10–12.

[3] Z. Lai and K. Lee, "Using unstable SRAM bits for physical unclonable function applications on off-the-shelf SRAM," in *Proc. IEEE Asia Pacific Conf. Circuits Syst. (APCCAS)*, Bangkok, Thailand, Nov. 2019, pp. 41–44, doi: 10.1109/APCCAS47518.2019.8953143.

[4] J. Trujillo, C. Merino, and P. Zarkesh-Ha, "SRAM physically unclonable functions implemented on silicon germanium," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Sapporo, Japan, 2019, pp. 1–4.

[5] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. Commun. Security*, Nov. 2002, pp. 148–160, doi: 10.1145/586110.586132.

[6] A. A. Zayed, H. H. Issa, and K. A. Shehata, "FinFET based low power ring oscillator physical unclonable functions," in *Proc. 31st Int. Conf. Microelectron. (ICM)*, Cairo, Egypt, Dec. 2019, pp. 227–230, doi: 10.1109/ICM48031.2019.9021283.

[7] N. A. Hazari, F. Alsulami, A. Oun, and M. Niamat, "Performance analysis of XOR-inverter based ring oscillator PUF for hardware security," in *Proc. IEEE Nat. Aerosp. Electron. Conf. (NAECON)*, Dayton, OH, USA, Jul. 2019, pp. 253–256, doi: 10.1109/NAECON46414.2019.9058002.

[8] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *Symp. VLSI Circuits. Dig. Tech. Papers*, Honolulu, HI, USA, 2004, pp. 176–179, doi: 10.1109/VLSIC.2004.1346548.

[9] K. T. Mursi, Y. Zhuang, M. S. Alkatheiri, and A. O. Aseeri, "Extensive examination of XOR arbiter PUFs as security primitives for resource-constrained IoT Devices," in *Proc. 17th Int. Conf. Privacy Security Trust (PST)*, Fredericton, NB, Canada, 2019, pp. 1–9.

[10] M. A. Alamro, Y. Zhuang, A. O. Aseeri, and M. S. Alkatheiri, "Examination of double arbiter PUFs on security against machine learning attacks," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Los Angeles, CA, USA, Dec. 2019, pp. 3165–3171, doi: 10.1109/BigData47090.2019.9006041.

[11] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proc. IEEE*, vol. 102, no. 8, pp. 1207–1228, Aug. 2014, doi: 10.1109/JPROC.2014.2332291.

[12] S. Ray, W. Chen, and R. Cammarota, "Protecting the supply chain for automotives and IoTs," in *Proc. 55th Annu. Design Autom. Conf.*, 2018, pp. 1–4, doi: 10.1145/3195970.3199851.

[13] D. Roy, J. H. Klootwijk, N. A. M. Verhaegh, H. H. A. J. Roosen, and R. A. M. Wolters, "Comb capacitor structures for on-chip physical uncloneable function," *IEEE Trans. Semicond. Manuf.*, vol. 22, no. 1, pp. 96–102, Feb. 2009, doi: 10.1109/TSM.2008.2010738.

[14] B. Škorić, S. Maubach, T. Kevenaar, and P. Tuyls, "Information-theoretic analysis of capacitive physical unclonable functions," *J. Appl. Phys.*, vol. 100, no. 2, pp. 24902–24911, Jul. 2006, doi: 10.1063/1.2209532.

[15] J. Biba, S. Boche, N.-H. Sadek, and W. Hansch, "Measurement setup for physical unclonable functions," in *Proc. 6th Int. Conf. Integr. Circuits Microsyst. (ICICM)*, 2021, pp. 155–159, doi: 10.1109/ICICM54364.2021.9660305.

[16] Ch. Böhm and M. Hofer, "Testing and specification of PUFs chapter 4," in *Physical Unclonable Functions in Theory and Practice*, 1st ed. New York, NY, USA: Springer-Verlag, 2013, pp. 69–86.

[17] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A large scale characterization of RO-PUF," in *Proc. IEEE Int. Symp. Hardw. Oriented Security Trust (HOST)*, 2010, pp. 94–99, doi: 10.1109/HST.2010.5513108.

[18] Z. Hu *et al.*, "Physically unclonable cryptographic primitives using self-assembled carbon nanotubes," *Nat. Nanotechnol.*, vol. 11, hboxpp. 559–565, Feb. 2016, doi: 10.1038/nnano.2016.1.

[19] B. Shao *et al.*, "Crypto primitive of MOCVD MoS^2 transistors for highly secured physical unclonable functions," *Nano Res.*, vol. 14, no. 6, pp. 1784–1788, 2021, doi: 10.1007/s12274-020-3033-0.

[20] J. Delvaux, D. Gu, I. Verbauwhede, M. Hiller, and M.-D. Yu, "Efficient fuzzy extraction of PUF -induced secrets: Theory and applications," in *Cryptographic Hardware and Embedded Systems (CHES)*, vol. 9813. Berlin, Germany: Springer, 2016, pp. 412–431. [Online]. Available: https://doi.org/10.1007/978-3-662-53140-2_20

[21] A. Mills, S. Vyas, M. Patterson, C. Sabotta, P. Jones, and J. Zambreno, "Design and evaluation of a delay-based FPGA physically unclonable function," in *Proc. IEEE 30th Int. Conf. Comput. Design (ICCD)*, 2012, pp. 143–146, doi: 10.1109/ICCD.2012.6378632.

[22] C. Böhm, M. Hofer, and W. Pribyl, "A microcontroller SRAM-PUF," in *Proc. 5th Int. Conf. Netw. Syst. Security*, 2011, pp. 269–273, doi: 10.1109/ICNSS.2011.6060013.

[23] M. Roel, "Physically unclonable functions: Constructions, properties and applications," Ph.D. dissertation, Dept. Electr. Eng., Katholieke Universiteit Leuven, Leuven, Belgium, 2012.