PUF-enabled Security Challenge
European Cyber Security Awareness Week (CSAW) 2023

Proposal of a new PUF based on sensors for the identification of IoT smart mobile devices

Raúl Aparicio-Téllez, Jorge Fernandez-Aragon, Abel Naya-Forcano and Guillermo Díez-Señorans

Supervisors: Miguel Garcia-Bosque, Santiago Celma

Group of Electronic Design (GDE), I3A, University of Zaragoza

Abstract: The increasing development of the Internet of Things (IoT) has suppose the exchange of large amounts of information among devices, that must be protected against cyberattacks. In this context, Physically Unclonable Functions (PUFs) arise as an optimal solution to this problem, as they exploit the stochastic variations occurring during the manufacturing process of the devices to generate a binary sequence that uniquely identifies each device. In this work, we propose a new PUF based on the signal measured by several sensors such as the accelerometer or the gyroscope of different smart mobile devices. This new proposal, designed exclusively for the participation in this competition, is especially interesting since using the sensors of the mobile devices does not require the implementation of additional electronic circuits, making the proposed PUF already integrated into an IoT system. The results obtained show that this PUF can be used for identification and authentication purposes, demonstrating that our solution can efficiently protect an IoT system.

Keywords: Authentication, hardware security, identification, internet of things, physically unclonable function.

1. Introduction

1.1. Justification of the use of PUFs in terms of security and system integration

One of the main challenges that the Internet of Things (IoT) must face is security. In these systems it is essential to protect the data to ensure that only authorized users can access to the information. Furthermore, IoT devices must meet certain requirements of size and power consumption. Nowadays, there are multiple security solutions for device authentication purposes based on generating a secret key and storing it in non-volatile memories (NVMs). However, storing sensitive data in NVMs makes systems susceptible to physical attacks [1, 2].

In this context, Physically Unclonable Functions (PUFs) arise as a promising solution. During the fabrication of integrated circuits, variations in silicon occur, making two apparently identical devices have some different properties. A PUF exploits these stochastic variations occurring during the manufacturing process to create unique key to authenticate each physical object, acting as the “fingerprint” of the device [3].

In terms of security, this approach is promising as the generated key is physically impossible to clone. Furthermore, it avoids storing secret information in NVMs as the key is only generated when it is necessary for a specific application, increasing the security of the systems. Furthermore, it reduces the cost of the devices since devices with NVMs are costly compared to those without NVMs. Typically, to integrate PUFs in IoT systems it is necessary to implement specific PUF architectures physically in Field-Programmable Gate Arrays (FPGAs) or Application-Specific Integrated Circuits (ASICs). However, we propose the utilization of certain sensors inherent to the devices to construct a PUF, so that it is not necessary to physically implement a specific security-circuit in the device, making the PUF already integrated in the system.

Nowadays, multiple types of PUF can be implemented including the *Arbiter* PUF [4], *Meta-stability* PUF [5] or *Ring-Oscillator* PUF [6]. In this work, we propose a novel PUF architecture to authenticate smart mobile devices based on the inherent sensors (accelerometer, gyroscope...) of these devices.

1.2. Justification of the type of the PUF primitive proposed

MEMS sensors are present in a large number of IoT devices, including mobile phones, tablets and smart watches. Among all the sensors that we can find in all these smart devices, two of them are fundamental for a wide range of applications: accelerometers and gyroscopes. On the one hand, accelerometers measure the linear acceleration of the device with respect to the acceleration of gravity. In a mobile device, these sensors can detect changes in the direction of movement or speed, and are used for various applications such as: step detection for health applications, device fall detection or device orientation detection. On the other hand, gyroscopes measure the angular velocity and allow devices to detect turns and rotational movements.

Since these sensors are built into most of the devices we use today, generating a key from them (that uniquely identifies each device) is promising as it would not be necessary to fabricate new electronic circuits solely for the purpose of generating a key, as it occurs in other types of PUFs. This means a cost reduction since it is not necessary to develop new physical circuits only for authentication purposes. In addition, MEMS sensors present a difficult-to-model behaviour, which makes a possible MEMS-PUF even more secure against modeling attacks.

The PUF proposal that we present in this works provides multiple advantages against possible security threats: firstly, the key is only generated when it is necessary to authenticate the device, preventing the key from being continuously exposed; secondly, it is already integrated into an IoT device that has its own security systems with the advantage that no external chip needs to be inserted with our solution; thirdly, in the situation that an attacker wants to attack the sensing layer, it would also necessary to know which parameters of the measured signal have been used to construct the PUF as well as how they have been estimated and encoded.

In this work, we propose the construction of a new PUF, designed exclusively for the participation in this competition, which is based on using some of the sensors present in the mobile devices that we all use daily [7]. This report is organized as follows. Section II explains the key metrics we have used to determine the quality of the PUF. Section III provides a technical description about the experiments as well as the steps we have followed to estimate the parameters given the raw data of the sensors. Section IV analyzes the properties of the proposed PUF. Finally, the conclusions are shown in Section V.

2. Attributes to characterize the PUF

Several properties must be evaluated to determine the quality of a PUF. Typically, the uniqueness and reproducibility are considered the most important ones. In this work, we have evaluated this properties using the Hamming Distance (*HD*) as a metric [1], defined as the number of different bits between two binary sequences Y and Y' of the same length n. Mathematically, it can be expressed as:

$$HD(Y, Y') = \sum_{i=1}^{n} Y_i \oplus Y'_i. \tag{1}$$

The distribution of the *HD* is typically modeled with a binomial distribution:

$$f_{binom}(k; n, p) = \binom{n}{k} p^k (1-p)^{n-k}. \tag{2}$$

A PUF should always provide the same response to the same challenge (reproducibility) in the same device and this response should be different from the response of other devices (uniqueness):

- **Uniqueness:** compares the responses produced by the same PUF in different devices. To evaluate the uniqueness of a PUF, the Inter-*HD* is used as metric. It measures the distance between the responses $Y_i(x)$, $Y_j(x)$ of the same PUF on two different devices $i \neq j$ under the same challenge x [1]:

  $$HD^{\text{inter}}_{i,j}(x) = HD(Y_i(x), Y_j(x)) \quad i \neq j. \tag{3}$$

  Ideally, the average Inter-*HD* should be 50%.

- **Reproducibility:** compares the responses produced by the same PUF in the same device in different instants. To evaluate the reproducibility, the Intra-*HD* is used as metric. It measures the distance between two responses $Y_j(x)$, $Y'_j(x)$ from a PUF on the device j under the same challenge x [1]:

  $$HD^{\text{intra}}_{j}(x) = HD(Y_j(x), Y'_j(x)). \tag{4}$$

  Ideally, all the Intra-*HD* should be 0%.

The main purpose of the proposed PUF in this work is the identification and authentication of devices. In a real identification system, it is evident that false rejections and false acceptances must be avoided. The probability of this happening is measured by the false rejection rate (*FRR*) and the false acceptance rate (*FAR*) [1]:

$$FRR(t_{id}) = 1 - F_{bino}(\hat{p}_P^{intra}) \tag{5}$$

$$FAR(t_{id}) = F_{bino}(\hat{p}_P^{inter}) \tag{6}$$

where $F_{bino}(\hat{p}_P^{intra})$ is the cumulative probability distribution (CDF) of the Intra-*HD*, and $F_{bino}(\hat{p}_P^{inter})$ is the CDF of the Inter-*HD*. *FAR* and *FRR* should be as small as possible, but they cannot be minimized at the same time. Typically, the identification threshold is chosen so as *FAR* and *FRR* are equal [1]. This point is called *equal error rate* threshold (t_{EER}) and the corresponding probability is the *equal error rate* (*EER*):

$$t_{EER} = \text{argmin}_t\{\max\{FAR(t_{id}), FRR(t_{id})\}\} \tag{7}$$

$$EER = \max\{FAR(t_{EER}), FRR(t_{EER})\}. \tag{8}$$

3. Technical description

3.1. PUF Proposal

Our experiments have been carried out using 8 smart mobile devices. Among the analyzed mobile devices, there are identical devices of the same manufacturer and model, devices of different models from the same manufacturer and devices from different manufacturers. Some of them use identical accelerometers and gyroscopes, while others use sensors with highly similar properties, most of them from STMicroelectronics, although some of them belong to Bosch Sensortec. Furthermore, five devices have an accelerometer and a gyroscope, while three have an accelerometer but not a gyroscope.

Firstly, we have placed the mobile devices on a flat surface and we have obtained the stationary acceleration and the angular velocity measured by the accelerometer and the gyroscope respectively. Ideally, since all the devices are stationary and parallel to the ground, we should read an acceleration value of 0 in the x and y axes, and a value of 9.8 m/s^2 in the z axis, corresponding to the acceleration of gravity. Regarding the gyroscope, it is evident that we should measure an angular velocity of 0 in all the three axes. However, in all accelerometers we have measured a non-zero acceleration in the x and y axes, and $\approx$ 9.8 m/s^2 in the z axis. Likewise, all gyroscopes measure a non-zero angular velocity. Figure 1 shows the measured acceleration in the x axis in one mobile device during 15 seconds using an accelerometer from STMicroelectronics. As it can be seen, the acceleration is measured with a certain level of noise. This phenomenon occurs for all the measured accelerations. Furthermore, in Figure 2 we show the acceleration measured in the x axis and the y axis, in the same conditions described before, for two identical mobile devices. As it can be seen, both signals provide a different value although they both belong to same-model devices, presenting a certain uniqueness.

In this work, we study the possibility of using some parameters derived from the signals obtained from the accelerometer and the gyroscope of the different mobile devices, with the objective of building a PUF for smart mobile authentication purposes. The measurements of acceleration have been carried out using a mobile app developed by our research group.

3.2. *Parameters of the accelerometer and gyroscope*

Among all the possible parameters that could be obtained from the signal measured with the accelerometer and the gyroscope, we have selected six potential parameters that could be used to build our PUF. The more parameters are used to build the PUF response, the better the system will be in terms of security. These six parameters are:

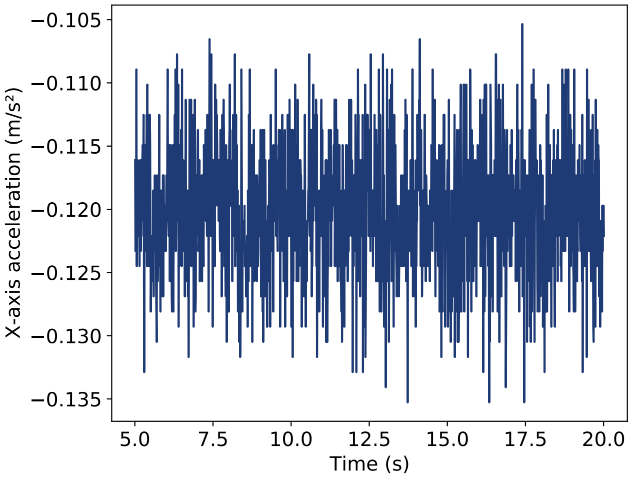


Figure 1. Acceleration measured in the x axis in one of the mobile devices.

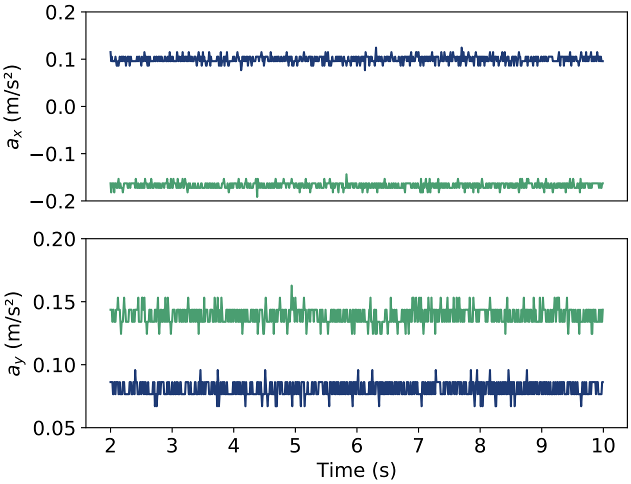


Figure 2. Comparison between the acceleration measured in the x axis and the y axis in two identical mobile devices under the same conditions.

(a) Accelerometer's average in $\hat{x}\hat{y}\hat{z}$ without vibration.
(b) Accelerometer's average in $\hat{x}\hat{y}\hat{z}$ with vibration.
(c) Gyroscope's average in $\hat{x}\hat{y}\hat{z}$ without vibration.
(d) Accelerometer's noise in $\hat{x}\hat{y}\hat{z}$ without vibration.
(e) Accelerometer's noise in $\hat{x}\hat{y}\hat{z}$ with vibration.
(f) Gyroscope's noise in $\hat{x}\hat{y}\hat{z}$ without vibration.

As it can be seen, four parameters correspond to the average value and the noise measured by the accelerometer and the gyroscope with the device stationary located in a flat surface without vibration. Furthermore, there are two extra parameters corresponding to the average value and the noise of the accelerometer while applying a vibration generated by the device.

Multiple approximations can be carried out to estimate the average and noise of both sensors. In this work, taking into account the computational cost and the precision that is necessary to achieve, to estimate these parameters we have divided the measured signal in N intervals. For each interval i, we have obtained the average value of the signal (γ^i_{aver}), the maximum value (γ^i_{max}) and the minimum value (γ^i_{min}). In this way, for each measurement, sensor, and axis, we have obtained three sequences of N numbers: $\{\Gamma_{aver}\}$, $\{\Gamma_{max}\}$, and $\{\Gamma_{min}\}$. For each sequence, we have obtained the average (μ) and the standard deviation (σ). Next, we have eliminated all values γ_i that are more than $k\cdot\sigma$ away from μ, keeping all values in the interval: $[\mu - k\cdot\sigma,\ \mu + k\cdot\sigma]$. In this way, we have obtained three new sets of numbers $\{\Omega_{aver}\}$, $\{\Omega_{max}\}$, and $\{\Omega_{min}\}$; each one defined based on $\{\Gamma_{aver}\}$, $\{\Gamma_{max}\}$, and $\{\Gamma_{min}\}$ respectively:

$$\{\Omega\} = \{\gamma_i \mid |\gamma_i - \mu| \leq k\cdot\sigma\} \tag{9}$$

To estimate the average and the noise without vibration, we have used $N = 10$ and $k = 3$. To estimate the average and the noise with vibration, we have used $N = 30$ and $k = 1$, as the signal is much more stable. Next, we have calculated the average of $\{\Omega_{aver}\}$, $\{\Omega_{max}\}$ and $\{\Omega_{min}\}$. Finally, given $\overline{\Omega_{aver}}$, $\overline{\Omega_{max}}$ and $\overline{\Omega_{min}}$, we have estimated the average ($\bar{s}$) and the noise (s_{noise}) of the signal:

$$\bar{s} = \overline{\Omega_{aver}}\ ,\ \ s_{noise} = |\overline{\Omega_{max}} - \overline{\Omega_{min}}| \tag{10}$$

Ideally, the accelerometer and the gyroscope measurements are done at complete rest. However, there are some external effects (small vibrations, touch of the screen...) that may appear, which occasionally could alter the acceleration or angular velocity measured. By eliminating all values outside the interval $[\mu - k\cdot\sigma,\ \mu + k\cdot\sigma]$, we are reducing or even eliminating the influence of all these effects on the estimation of $\bar{s}$ and s_{noise}. Given $\bar{s}$ and s_{noise}, we have obtained two numbers α and α_{noise} in the interval $(-100, 100)$ for each axis and each one of these cases: (1) accelerometer with vibration, (2) accelerometer without vibration y (3) gyroscope without vibration:

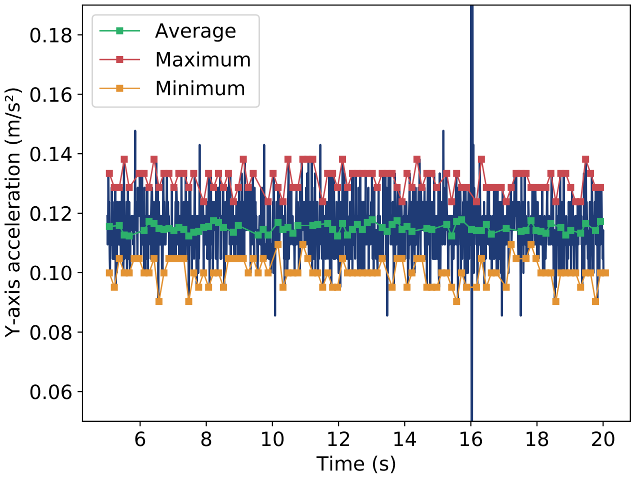


Figure 3. Estimation of α and α_{noise} using the signal of one accelerometer without vibration.

$$\alpha = \bar{s}\cdot 10^{\delta} \qquad \alpha_{noise} = s_{noise}\cdot 10^{\delta} \tag{11}$$

where $\delta = 2$ for the parameters (a), (b) and (e); $\delta = 3$ for (d); $\delta = 4$ for (f) and $\delta = 5$ for (c).

In Figure 3, the acceleration measurements made by the accelerometer without vibration during 15 seconds in one device are shown. Likewise, the values that have been used to estimate the mean and the noise of the signal are also shown. In this case, the first 5 seconds have been discarded in order to stabilize the measured signal. As it can be seen, at $t = 16$ s the acceleration suddenly increases. This corresponds to a touch on the screen of the device. However, using the proposed method to estimate $\bar{s}$ and s_{noise}, this effect is not taken into account. In this example, after this process, we have estimated $\bar{s} = 0.1149$ m/s^2 and $s_{noise} = 0.0308$ m/s^2, thus obtaining $\alpha = 11$ and $\alpha_{noise} = 31$.

3.3. Encoding process

As previously explained, using the described method we have obtained a number in $(-100, 100)$ for each parameter and device. However, it is more convenient to convert the integer to a binary sequence, as it helps to correct some errors and is required by some communication standards and protocols. To carry out this encoding process we could directly use the Binary-Coded Decimal (BCD) standard, in which each digit is assigned a sequence of four bits. However, this encoding process is not stable facing process variations. Therefore, we have transformed each α and α_{noise} into a binary sequence using the Gray Code. In this coding standard, only one bit changes between two consecutive numbers. This is especially interesting for our application, since the response obtained in the device will be more stable facing changes in the operating environment thus reducing the HD of sequences corresponding to the same device. For example, consider two time instants t, t' where $\alpha(t) = 7$ and $\alpha(t') = 8$. Using the BCD standard, we obtain: $HD = 4$, while using the Gray Code: $HD = 1$.

However, we have observed that (some) numbers tend to appear more than others. In Figure 4, we have represented all α and α_{noise} parameters obtained for each device. As it can be seen, most of the parameters usually have values between -17 and 54. This means that for numbers in $[-17,\ 54]$ it is necessary to obtain a higher precision compared to numbers outside that interval. For this purpose, instead of assigning directly to each decimal number its corresponding gray code, we have fitted the data to a Gaussian distribution and have divided the distribution into intervals of equal probability [8]. To each one of these intervals, a 6-bit sequence has been assigned according to the gray code. In this way, once α and α_{noise} are obtained, we observe in which interval the number falls and the corresponding 6-bit sequence is assigned.

3.4. Obtaining the PUF response

For each parameter, axis and device, a sequence of 6 bits is obtained. To obtain the final sequence for each device, we have joined together all the values obtained (Figure 5). In this way, we have obtained sequences up to 6 parameters × 3 axes × 6 bits $=$ 108 bits for each device. In case of devices without gyroscope, a 72-bit word is obtained.

3.5. Integration in an IoT system

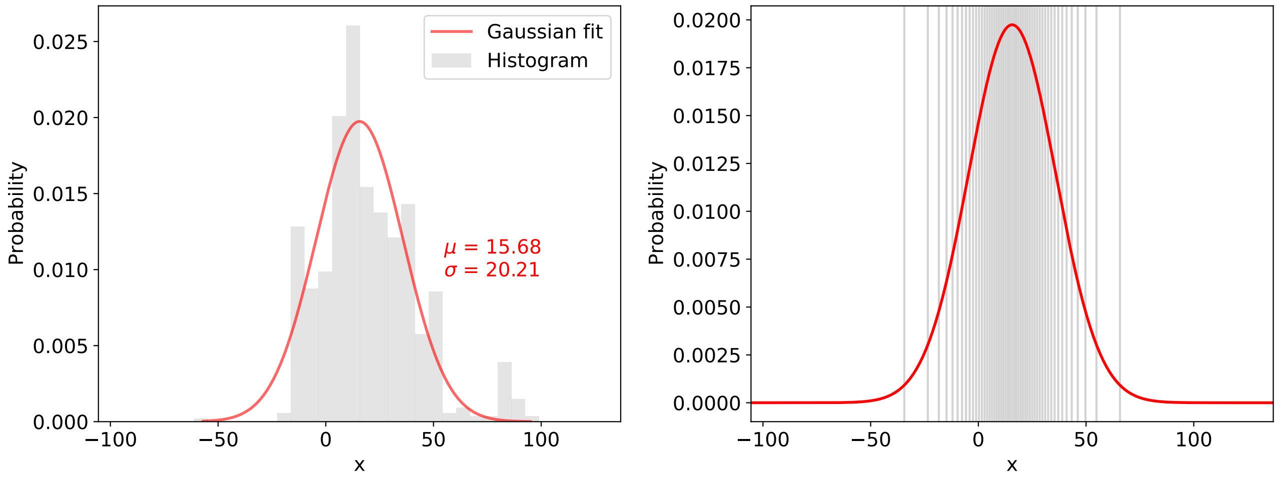
Accelerometers and gyroscopes are present in most wearable smart devices, including mobile phones, tablets, smartwatches... Likewise, they are also used in the industrial machinery, medical environments, and sensor networks to collect information through sensors strategically distributed in certain locations. For this reason, the main advantage of our PUF proposal is that it is already integrated in an IoT system and it does not require the implementation of any extra sensor or any additional electronic circuit, reducing significantly the cost of the devices.

Furthermore, to make the PUF proposal fully integrated in an existing IoT system, we have developed a prototype of an app for Android used to generate the 108-bit key of the devices. The application measures the acceleration and angular velocity of the phone during a certain time interval under the conditions described above. Next, it estimates the 6 parameters described and displays the binary sequence on the screen. This key is unique for each mobile and uniquely identifies the device. In Figure 6, we show a screenshot of the described app.

4. Analysis of the PUF properties

4.1. Using the response of the accelerometer

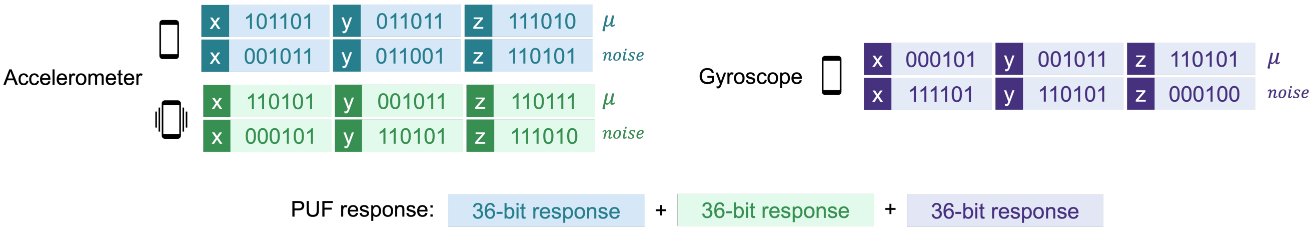
In Figure 7, we have represented the estimated noise values $\bar{s}$ and s_{noise} of the accelerometer with vibration and without vibration throughout 10 repetitions. The measurements have been carried out at different instants and in different surfaces. As it can be seen, a certain PUF behavior can be intuited in the analyzed parameters, since the measured variables are approximately stable with respect to the number of repetitions and, in addition, the parameters obtained are different for all devices. Furthermore, we have also represented the estimated average values of the accelerometer with vibration and without vibration. Again, there is a certain uniqueness in the values obtained, as they are different from one device to another; and there is also a certain reproducibility, as in the majority of the cases this value can be repeated throughout the measurements.



(a) Gaussian fit.

(b) Gaussian segmentation in intervals with equal probability.

Figure 4. Encoding process using a Gaussian distribution in the interval $[\mu - 5\sigma, \mu + 5\sigma]$.



Accelerometer

x 101101 y 011011 z 111010 μ
x 001011 y 011001 z 110101 *noise*

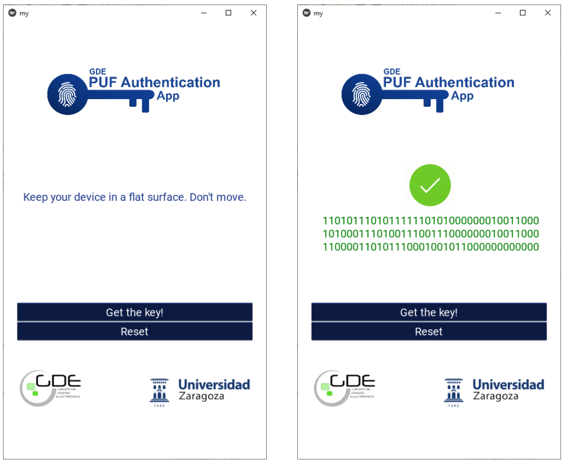
x 110101 y 001011 z 110111 μ
x 000101 y 110101 z 111010 *noise*

Gyroscope

x 000101 y 001011 z 110101 μ
x 111101 y 110101 z 000100 *noise*

PUF response: 36-bit response + 36-bit response + 36-bit response

Figure 5. Process to obtain the PUF response.



Keep your device in a flat surface. Don't move.

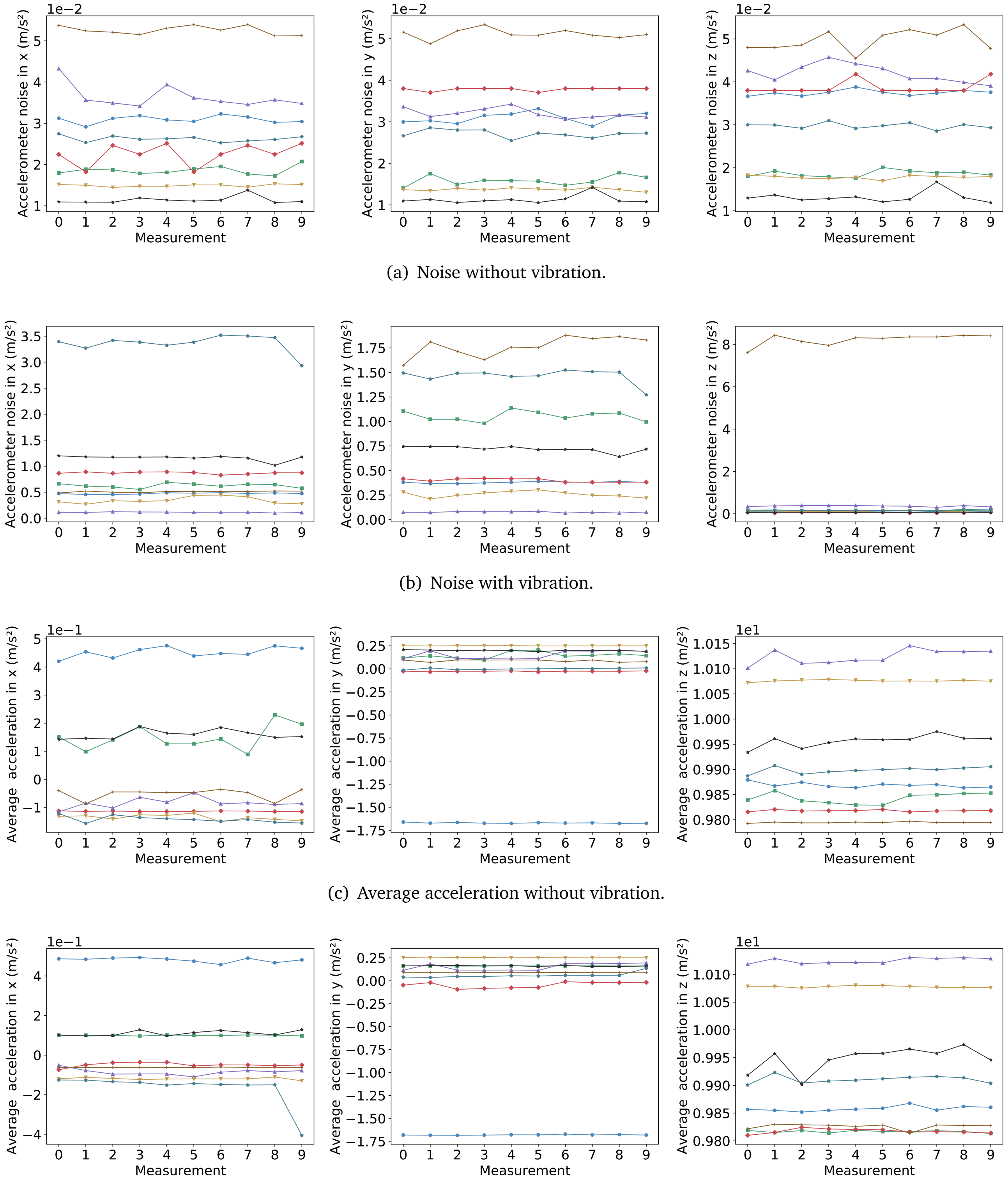
110101110101111110101000000010011000
101000111010011100111000000010011000
110000110101110001001011000000000000

(a) Before key generation (b) After key generation

Figure 6. App screenshot before and after the key generation.

Next, we have obtained α and α_{noise} and thus the 72-bit binary sequence. Then, we have used the 72-bit responses to construct a PUF. To determine the reproducibility of the proposed PUF, we have obtained the 72-bit response 10 times and have obtained the Intra-*HD* distribution for each device.

Then, we have obtained the average Intra-*HD* for each device μ_i^{intra} and the average Intra-*HD* for all distributions $\overline{\mu^{intra}} = \sum_i \mu_i^{intra} = 13.25\%$. To determine the uniqueness of the PUF, we have compared the responses generated by each device and have obtained the Inter-*HD* distribution. We have obtained an average Inter-*HD* of $\mu^{inter} = 46.13\%$. Figure 8 shows the Intra-*HD* distribution obtained for one of the devices together with the Inter-*HD* distribution. As it can be seen, the proposed PUF exhibits a certain degree of identifiability since the Inter-*HD* distribution is higher than the Intra-*HD* distribution. This occurs for all scanned devices and indicates that it is possible to use our PUF for device identification and



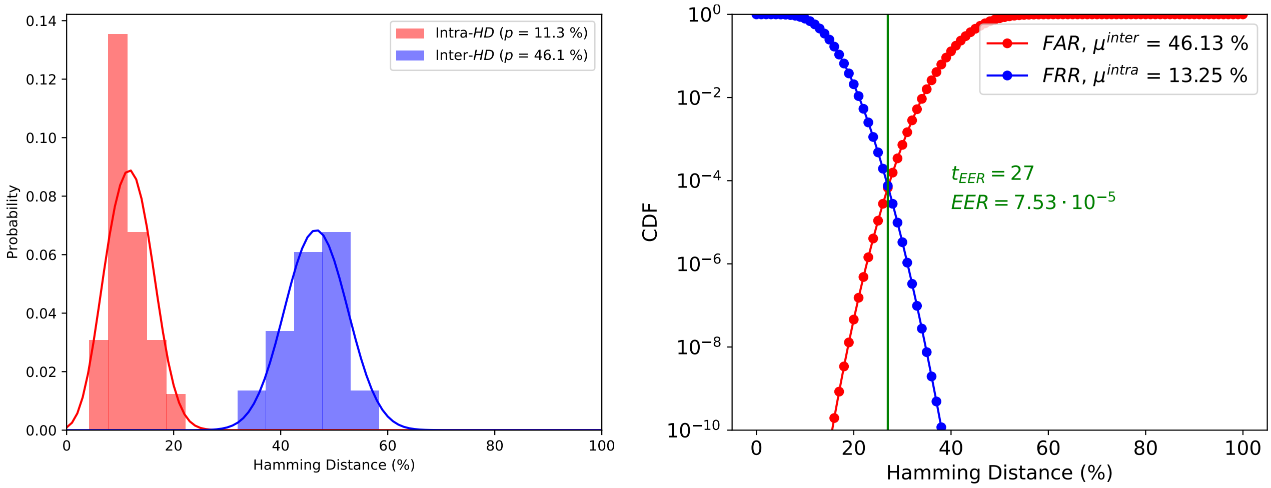
(a) Noise without vibration.

(b) Noise with vibration.

(c) Average acceleration without vibration.

(d) Average acceleration with vibration.

Figure 7. Parameters obtained from the accelerometer. Each symbol/line corresponds to a different mobile device.



(a) Inter-*HD* and Intra-*HD* distributions

(b) *FAR* and *FRR* distributions

Figure 8. Uniqueness, reproducibility and identifiability using the responses of the accelerometer.

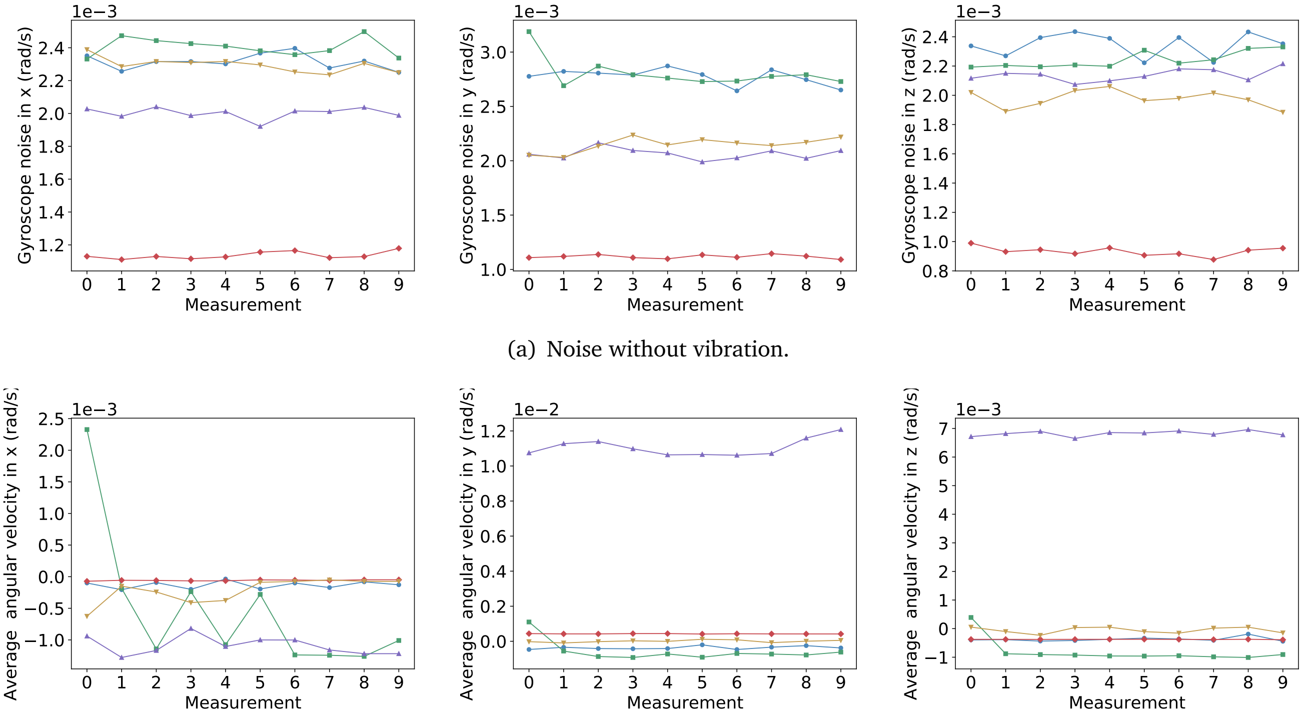
authentication purposes.

Finally, we have carried out an identifiability analysis. With this purpose, we have fitted the Intra-*HD* and Inter-*HD* to binomial distributions and we have calculated the *FAR* and *FRR* curves given the binomial fits. Both *FAR* and *FRR* are shown in Figure 8. Furthermore, we have obtained the equal error rate and the equal error threshold: $EER(t_{EER} = 27) = 7.53 \cdot 10^{-5}$. This means that only $\approx 0.008\%$ of the device identification attempts will result in a false rejection or a false acceptance, and that therefore the proposed PUF, using only the accelerometer, could be effectively used for the authentication of smart mobile devices.

4.2. *Combining the response of the accelerometer and gyroscope*

Again, we have obtained the average angular velocity and the noise measured by the gyroscope of the devices throughout 10 repetitions. In Figure 9, we have represented the parameters $\bar{s}$ and s_{noise} measured with the gyroscope for the three axes xyz. As it can be seen, a certain PUF behavior is observed, since $\bar{s}$ and s_{noise} are approximately stable during the 10 measurements and there is also a difference between the values obtained from one device to another.

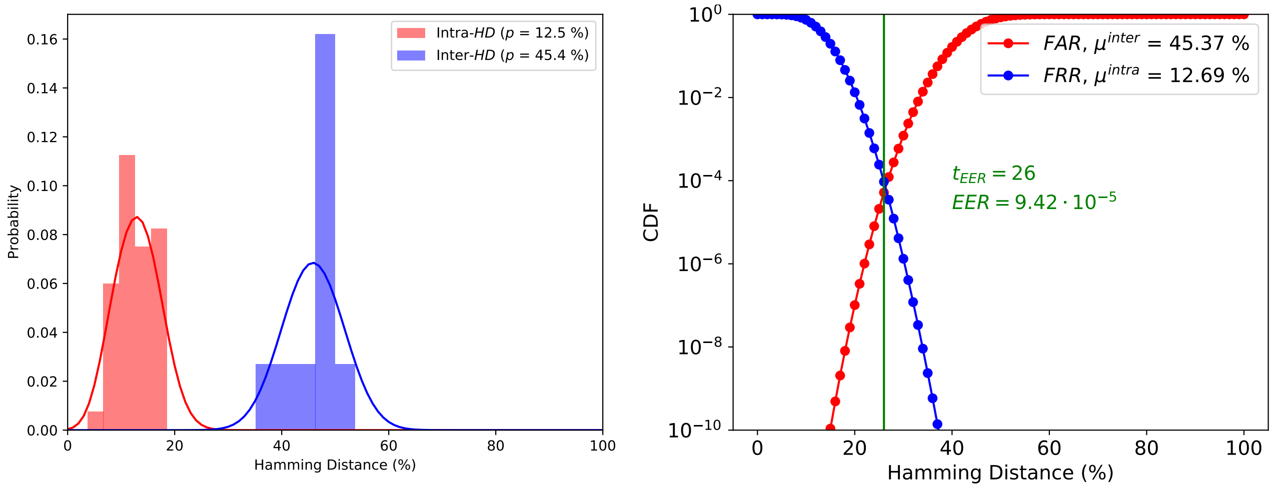
Subsequently, we have combined the 72-bit response obtained using the accelerometer with the 36-bit response using the gyroscope, thus obtaining a 108-bit response for each device. To determine the reproducibility of this PUF, we have taken 10 measurements on each of the devices and have calculated the Intra-*HD* distribution for each of the devices. Then, we have obtained the average Intra-*HD* for each device μ_i^{intra} and the average Intra-*HD* for all distributions $\overline{\mu^{intra}} = 12.69\%$. To determine the uniqueness of the PUF, we have compared the responses generated by each one of the devices and we have obtained the Inter-*HD* distribution. In this case, we have obtained an average Inter-*HD* of $\mu^{inter} = 45.37\%$. In Figure 10, we have represented the Intra-*HD* distribution obtained for one of the devices together with the Inter-*HD* distribution. As it can be seen, the proposed PUF exhibits a certain degree of identifiability, since the Inter-*HD* distribution obtained is higher than the Intra-*HD* distribution. This occurs for all scanned devices and indicates that it is possible to use the PUF proposal for device identification and authentication purposes. Comparing the properties of this PUF with the properties of the PUF using only the response of the accelerometer, the reproducibility, the uniqueness and therefore the identifiability is improved by using the key generated by the gyroscope.



(a) Noise without vibration.

(b) Average angular velocity without vibration.

Figure 9. Parameters obtained from the gyroscope.



(a) Inter-*HD* and Intra-*HD* distributions

(b) *FAR* and *FRR* distribution

Figure 10. Uniqueness, reproducibility and identifiability of the PUF combining the responses of the accelerometer and the gyroscope.

Finally, we have carried out an identifiability analysis. With this purpose, we have calculated the *FAR* and *FRR* curves given the binomial fits of the Intra-*HD* and Inter-*HD* distributions. Both distributions are shown in Figure 10. Furthermore, we have obtained the equal error rate and the equal error threshold: $EER(t_{EER} = 26) = 9.42 \cdot 10^{-5}$. This means that only ≈ 0.009% of the device identification attempts will result in a false rejection or a false acceptance, and that therefore the proposed PUF using the responses of the accelerometer and the gyroscope combined can be used for smart mobile device authentication purposes.

4.3. Security threats addressed by the PUF-based security feature

IoT systems must face many security threats [9, 10]. The lack of strong identification and effective authorization systems makes these devices vulnerable to unauthorized accesses. Each layer in an IoT system is a security threat that must be avoided. Security attacks can be produced in the sensing layer, network layer, gateway, or application layer [11].

The proposed PUF helps to resolve some security threats present in some of these layers of IoT systems. MEMS sensors exhibit a difficult-to-model behavior, making our PUF robust against possible modeling attacks. In addition, it also obstructs possible attacks occurring in the sensing layer, since although a possible attacker has physical access to the sensors, the mobile device must be in a certain position and state to obtain the response of the PUF. In particular, within the sensing layer, our PUF would also hinder possible side channel attacks, since to obtain the PUF response it is necessary for the accelerometer and gyroscope to reach a certain steady state where the signal is stable. That is the reason why some previous seconds are eliminated to estimate the average and noise. Furthermore if the attacker manages to intercept the acceleration and angular velocity data, it would still be necessary to know the size of the intervals and the number of sigmas to make the estimation of the average and the noise. Likewise, if known the size of the intervals and number of sigmas, it would still be necessary to know how the Gaussian encoding process is done. And even the Gaussian encoding process is known, it remains necessary to know how the responses of the different parameters and axes are combined to generate the response.

Therefore, our PUF, in addition to reducing the cost of devices by using sensors that they already have incorporated, helps solve or minimize some security threats of IoT systems.

5. Conclusions

In this work, we have proposed a new architecture of PUF based on the accelerometer and the gyroscope of mobile smart devices. Firstly, we have observed that the accelerometer and the gyroscope provide a non-zero with a certain level of noise when placed stationary in a flat surface. Furthermore, we show that the noise and the non-zero value can be used to construct a PUF. Then, we introduce a new approach to estimate both parameters given the measured signal as well as a new method to encode the measured value into a binary sequence.

Moreover, we have analyzed the response of a PUF which uses the average and the noise of the accelerometer with and without vibration applied to the device. The results obtained show a certain PUF behaviour as the Inter-*HD* distribution obtained is significantly higher than the Intra-*HD* distribution. In terms of identifiability, we have obtained an $EER = 7.53 \cdot 10^{-5}$ using only the accelerometer and $EER = 9.42 \cdot 10^{-5}$ if we introduce the response obtained from the gyroscope. These results show that our proposed PUF can be used to authenticate the mobile devices, demonstrating that this approach can efficiently used to protect an IoT system.

Future lines of research may include to increase the number of devices used, adjust the specifications used to make the estimation of the six parameters proposed, study the possibility of using other sensors, and extract new parameters given the signals of the accelerometer and the gyroscope.

References

[1] Roel Maes. *Physically Unclonable Functions : Constructions, Properties and Applications*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013 edition, 2013.

[2] Charles Herder, Meng-Day Yu, Farinaz Koushanfar, and Srinivas Devadas. Physical Unclonable Functions and Applications: A Tutorial. *Proceedings of the IEEE*, 102(8):1126–1141, 2014.

[3] Christoph Böhm and Maximilian Hofer. *Physical Unclonable Functions in Theory and Practice*. Springer, New York, NY, 2013.

[4] Zhangqing He, Wanbo Chen, Lingchao Zhang, Gaojun Chi, Qi Gao, and Lein Harn. A Highly Reliable Arbiter PUF With Improved Uniqueness in FPGA Implementation Using Bit-Self-Test. *IEEE Access*, 8:181751–181762, 2020.

[5] Ying Su, Jeremy Holleman, and Brian P. Otis. A Digital 1.6 pJ/bit Chip Identification Circuit Using Process Variations. *IEEE Journal of Solid-State Circuits*, 43(1):69–77, 2008.

[6] Raúl Aparicio-Téllez, Miguel Garcia-Bosque, Guillermo Díez-Señorans, and Santiago Celma. Oscillator Selection Strategies to Optimize a Physically Unclonable Function for IoT Systems Security. *Sensors*, 23(9), 2023.

[7] Saeed Abdolinezhad, Axel Sikora, and Achim Bittner. Design, simulation, and analysis of physical unclonable functions with mems aln cantilevers. In *2022 Smart Systems Integration (SSI)*, pages 1–6, 2022.

[8] Oliver Willers, Christopher Huth, Jorge Guajardo, and Helmut Seidel. Mems gyroscopes as physical unclonable functions. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, page 591602, New York, NY, USA, 2016. Association for Computing Machinery.

[9] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, and Faiz Alotaibi. Internet of things security: A survey. *Journal of Network and Computer Applications*, 88:10–28, 2017.

[10] Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, and Biplab Sikdar. A survey on iot security: Application areas, security threats, and solution architectures. *IEEE Access*, 7:82721–82743, 2019.

[11] Saloni Bansal and V.K Tomar. Challenges and security threats in iot with solution architectures. In *2022 2nd International Conference on Power Electronics and IoT Applications in Renewable Energy and its Control (PARC)*, pages 1–5, 2022.