Design of hardware-based security solutions for interconnected systems

Miguel Ángel Prada Delgado

Department of Electronics and Electromagnetism
Physical Sciences and Technologies (PS&T) Doctoral Programme
University of Seville

This dissertation is submitted for the degree of
Doctor by the University of Seville with international mention

Seville Institute of Microelectronics
(IMSE-CNM)

September 2019

Everything we hear is an opinion, not a fact. Everything we see is a perspective, not the truth.

Marco Aurelio

Acknowledgements

First of all, I would like to acknowledge my advisor, Iluminada Baturone, for always being open to help and guide me throughout every challenge we have encountered. Without her unlimited patience and willingness to always go the extra mile, the results of this thesis would not have been possible.

I would also like to thank the Institute of Microelectronics of Seville (IMSE-CNM) for hosting me for so many years. This center has been like my second home, and I have had the pleasure of sharing fantastic experiences with great colleagues. Thanks to Alfredo Vazquez, Javier Arcenegui, Macarena Martínez, Rosario Arjona, and Susana Eiroa, as well as the rest of my group for their invaluable contributions during our joint research.

Thanks also to my office mates, Laurentiu Acasandrei, Angela Darie, and James Romaine, for the great moments we have spent together both professional and personal. I could not have had a better working environment.

Regarding my doctoral stays, I would like to thank Jose Manuel Martínez who hosted me at the Harvard RCC, and Andreas Kind, Gero Dittmann, and Jens Jelitto, who welcomed me at the IBM Zurich Research Lab, as well as the working groups in both centers. I much appreciate you allowed me to collaborate and work with you.

Last but not least, I would like to thank my wife, Anastasia, for her unconditional support, as well as my parents, Ángel and Antonia, my brother, Javier, and the rest of my family for helping me get where I am today. None of these would have been possible without them.

Abstract

Among all the different research lines related to hardware security, there is a particular topic that strikingly attracts attention. That topic is the research regarding the so-called Physical Unclonable Functions (PUF). The PUFs, as can be seen throughout the Thesis, present the novel idea of connecting digital values uniquely to a physical entity, just as human biometrics does, but with electronic devices. This beautiful idea is not free of obstacles, and is the core of this Thesis. It is studied from different angles in order to better understand, in particular, SRAM PUFs, and to be able to integrate them into complex systems that expand their potential.

During Chapter 1, the PUFs, their properties and their main characteristics are defined. In addition, the different types of PUFs, and their main applications in the field of security are also summarized.

Once we know what a PUF is, and the types of them we can find, throughout Chapter 2 an exhaustive analysis of the SRAM PUFs is carried out, given the wide availability of SRAMs today in most electronic circuits (which dramatically reduces the cost of deploying any solution). An algorithm is proposed to improve the characteristics of SRAM PUFs, both to generate identifiers and to generate random numbers, simultaneously. The results of this Chapter demonstrates the feasibility of implementing the algorithm, so in the following Chapters it is explored its integration in both hardware and software systems.

In Chapter 3 the hardware design and integration of the algorithm introduced in Chapter 2 is described. The design is presented together with some examples of use that demonstrate the possible practical realizations in VLSI designs.

In an analogous way, in Chapter 4 the software design and integration of the algorithm introduced in Chapter 2 is described. The design is presented together with some examples of use that demonstrate the possible practical realizations in low-power IoT devices. The algorithm is also described as part of a secure firmware update protocol that has been designed to be resistant to most current attacks, ensuring the integrity and trustworthiness of the updated firmware.

In Chapter 5, following the integration of PUF-based solutions into protocols, PUFs are used as part of an authentication protocol that uses zero-knowledge proofs. The cryptographic protocol is a Lattice-based post-quantum protocol that guarantees the integrity and anonymity of the identity generated by the PUF. This type of architecture prevents any type of impersonation or virtual copy of the PUF, since this is unknown and never leaves the device. Specifically, this type of design has been carried out with the aim of having traceability of identities without ever knowing the identity behind, which is very interesting for blockchain technologies.

Finally, in Chapter 6 a new type of PUF, named as BPUF (Behavioral and Physical Unclonable Function), is proposed and analyzed according to the definitions given in Chapter 1. This new type of PUF significantly changes the metrics and concepts to which we were used to in previous Chapters. A new multi-modal authentication protocol is presented in this Chapter, taking advantage of the challenge-response tuples of BPUFs. An example of BPUFs is illustrated with SRAMs.

A proposal to integrate the BPUFs described in Chapter 6 into the protocol of Chapter 5, as well as the final remarks of the Thesis, can be found in Chapter 7.

Table of contents

List of figures

List of tables

Chapter 1

Introduction

1.1 Physical unclonable functions (PUFs)

The concept of a *physical unclonable function* (PUF) is difficult to describe in a single closed definition. Some attempts to define a PUF exclude certain types of PUFs or include other things besides PUFs.

First, we will make a list of the most important properties that come from different definition attempts identified in the PUFs proposals [1–4].

To simplify the description of the properties, we start from a basic definition of a PUF as a physical challenge-response procedure. It should be taken into account that this assigns implicitly two properties to PUFs, i.e., the instantiation of a PUF cannot simply be an abstract concept, but it is always integrated into a physical entity, and PUF is a procedure (not strictly a function) with some input and output functionalities. Since these properties are fundamental and are immediately clear from the construction of all the PUFs proposed so far, they will not be discussed. For ease, the notation: $\Pi : X \to Y : \Pi(x) = y$ is used to denote the challenge-response functionality of a PUF Π.

We begin by listing seven recurring properties identified from multiple attempts to define the PUFs, completely formal properties. The informal parts of the property descriptions are clearly shown in *italics*.

1. **Evaluable**: Given Π and x, it is *easy* to evaluate $y = \Pi(x)$.

2. **Unique**: $\Pi(x)$ contains *some* information about the identity of the physical entity integrated in Π.

3. **Repeatable or reproducible**: $y = \Pi(x)$ is reproducible with a *small error*.

4. **Unclonable**: Given Π, it is *difficult* to build a procedure $\Gamma \neq \Pi$ such that $\forall x \in X$: $\Gamma(x) \approx \Pi(x)$ with *a small error*.

5. **Unpredictable**: Given only one set $Q = (x_i, y_i = \Pi(x_i))$, it is *difficult* to predict $y_c \approx \Pi(x_c)$ with a *small error*, for x_c a random challenge such that $(x_c, \cdot) \notin Q$.

6. **Unique direction**: Given only y and Π, it is *difficult* to find x such that $\Pi(x) = y$.

7. **Obvious alteration**: An alteration of the integrated physical entity Π transforms Π into Π' such that with a *great probability* $\exists x \in X / \Pi(x)$ is *greatly different* from $\Pi'(x)$.

After this, we will discuss in more detail the seven properties:

1. Whether a PUF is evaluable or not can be interpreted in a very general way. From a theoretical perspective, *easy* can mean that we want the evaluation to be possible in polynomial time and effort. From a practical point of view, this means that the evaluation that induces the lowest possible overload is desired, for example, given the time, area, power and energy restrictions of an integrated circuit. It should also be noted that if the PUF is evaluable, it is implicit that it should be simple its fabrication.

2. Regarding the description of the property of uniqueness, if a well-defined set or population of PUF instances is considered, the information contained in a response of the PUF $\Pi(x)$ allows selecting a partition of the population, with the PUF instances able to provide that response. Successive responses allow having smaller and smaller partitions of the population until only a single instantiation of the PUF is optimal, in which case the set of unique responses identifies the PUF in the population. Based on the size of the population and the characteristics of the PUF response, such a unique identification may or may not be possible. A possible measure of the uniqueness that is provided in most experimental results is the Inter-Class Hamming distance histogram, obtained from the Inter-Class Hamming distance histogram, in particular from its average value of $avg_{InterHD}$.

3. The property of repeatability or reproducibility is clear from its description. The responses to the different evaluations of the same challenge x in the same PUF Π must be close in the considered metric distance. For experimental results, this is measured from the Intra Hamming distance histogram, in particular from its average value $avg_{InterHD}$. Reproducibility is the characteristic that distinguishes PUFs from true random number generators (TRNGs).

4. As can be expected from its name, unclonability is the main property of a PUF. The description provided is relatively obvious, however, there are many details that

should be taken into consideration. First, if it is difficult to reach a physical entity that contains another PUF $\Pi_\Gamma \neq \Pi$ such that $\forall x : \Pi_\Gamma(x) \approx \Pi(x)$. We say that Π is not physically clonable. The difficulty of producing a physical copy exists even for the manufacturer of the original PUF Π. That is why this property is also called manufacturer resistance. If it is difficult to find a mathematical procedure (abstract) f_Γ such that $\forall x : f_\Gamma(x) \approx \Pi(x)$, we say that Π is not mathematically clonable. The physical and mathematical unclonability have different properties, since the construction can be easy to copy physically but not mathematically, and vice versa. In order to be truly unclonable, Π has to be both physically and mathematically unclonable. Once again, the *difficulty* of cloning can be considered from a theoretical and a practical point of view. In practice, cloning can be very difficult or unfeasible. On the other side, proving the theoretical unclonability is very difficult. The only known system that can be proved as theoretically unclonable is based on quantum physics.

5. Unpredictability is in fact a relaxed form of unclonability. If you can correctly predict the outcome of a PUF for a random challenge, only from observing a set of responses, it is easy to build a mathematical clone if you have access to the full PUF. Therefore, predictability implies mathematical clonability, and consequently clonability [1].

6. Unidirectionality is a classic property derived from cryptography. The first definition of PUF describes them as a physical variant of one-way functions.

7. Over time, a number of notions were proposed in the literature in relation to manipulation and security against manipulation. As an alteration or manipulation, we understand the realization of permanent changes to the integrity of the physical entity. We will call evident manipulation of the PUF to the manipulation of the physical entity integrated in the PUF, which with high probability changes the behavior of the PUF response.

1.2 Types of PUFs

In this section a list of the possible PUFs by category is presented, distinguished basically by their construction and operating principles. It should be noted that we will not go into detail in PUFs that do not have a direct relationship with this document, but rather we will focus on memory-based PUFs. On the rest of these PUFs you can find information on [3].

1.2.1 Non-electronic PUFs

In this section we will mention some PUFs that are not based on inherently electronic designs. However, electronic and digital techniques are often used to store the response of the PUFs efficiently. Therefore, the common denomination as non-electronic PUFs only indicates that the random nature that makes the PUF unique is not electronic, but does not imply that there is no subsequent measurement, storage and electronic processing. Some of these PUFs are:

1. **Optical PUFs**: They use a sample with an optical microstructure of refracting glass spheres in a transparent epoxy base. After irradiating the sample with a helium-neon laser, they produce a pattern due to scattering that is captured by a CCD sensor and processed by computer. The pattern obtained depends on the angle of incidence of the laser beam, so the challenge of this PUF is described by a precise laser incidence angle and the output pattern due to scattering.

2. **Paper PUFs**: We call paper PUFs those that consist in scanning the unique and random fiber structure of a normal or modified paper. The reflection of light from the paper is measured when a laser beam (for example, from a normal scanner) impinges on it to prevent its falsification.

3. **CDs PUFs**: There is a measurable deviation by a conventional CD player in the expected lengths of the valleys and ridges of the CDs, being unique in each CD.

4. **Radiofrequency PUFs**: The same sample is used as for the optical PUFs, except that the incident signal is of radio frequency and the pattern of electromagnetic radiation emitted by the dispersion is measured.

5. **Magnetic PUFs**: Use the uniqueness of particle patterns in magnetic media, such as credit cards.

6. **Acoustic PUFs**: Acoustic delay lines are used to delay electrical signals. The PUF is based on observing the alteration and the delay produced by these lines in the frequency spectrum.

1.2.2 Analog electronic PUFs

This section will list some PUFs that consist of the measurement of some electrical or electronic quantity. Some of them are [3, 4]:

1. V_T **PUFs**: They are based on measuring the charge of a capacitor due to the voltage V_T of each transistor, which is partially random due to the manufacturing process.

2. **Power distribution PUFs**: They are based on the variation of the resistance of the power supply network of a chip. Each power supply network is different and depends on the manufacturing process.

3. **Layer PUFs**: They measure the variation of the capacity of a sensor in the form of a comb in the upper layer of an integrated circuit. Randomness is introduced explicitly by means of a passive dielectric sprayed on the upper layer of the sensors.

4. **LC PUFs**: The LC PUFs are constructed with a glass plate and two metal plates, one on each side forming a capacitor connected in series with a metal coil. Together they form a passive LC circuit that stores energy inside an RF field. After a frequency scan, the resonance frequency is obtained, which is unique due to the fabrication.

1.2.3 Intrinsic PUFs based on delay

They are based in principle on the analogical measurement of a random physical parameter, which is later quantized and used to identify the whole system. To denominate intrinsic to a PUF it must fulfill that the PUF and the elements of measure are integrated in the device, as well as that the PUF construction must consist of procedures and primitives that are available naturally in the manufacturing process of the integrated device. Again, we list some of them [3, 4]:

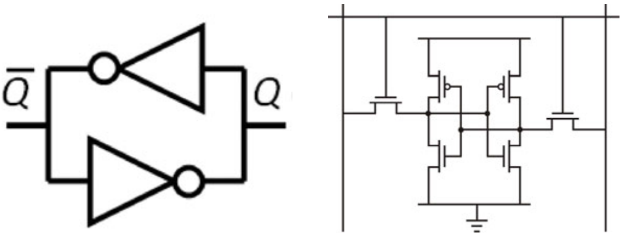
1. **Arbiter PUFs**: The main idea is to introduce a digital competition condition by two paths on a chip, and have an arbiter decide which of the two paths *wins* the race. If the two paths are symmetrical you can not know in advance which will be faster because the difference will depend on the physical parameters of manufacture. The paths must be long enough so that they do not violate the setup and hold time of the arbiter.

2. **Ring oscillator PUFs**: The ring oscillators work with inverters that feed the output with the input, inverting it asynchronously. The result is an output signal that oscillates at a frequency dependent on the delay of the inverter line. The PUFs based on ring oscillators measure the deviation of this frequency caused by manufacturing variations.

1.2.4 Memory-based intrinsic PUFs

In this section we will talk about the PUFs that are most related to this Thesis. A digital memory cell is typically a digital circuit that can be found in more than one stable state. In one of those states, the cell stores information (a binary digit, bit, in case of having two states). However, if it is used in a state of unstability, it is not known with certainty what value it will take when it stabilizes. Some cells have a tendency to always take a concrete state. This is due to variations in the manufacturing process, so we can use this information as a PUF. Based on this principle, we can distinguish some PUFs like the ones listed below [3, 4]:

1. **SRAM PUFs**: SRAMs (or Static Random-Access Memories) are formed by cells, each of which can store a binary digit. As shown in Figure 1.1(a), the cells are formed by two inverters fed back to each other. In conventional CMOS technology, these inverters are implemented with four transistors as shown in the Figure 1.1(b). It is not known with certainty when the SRAM memory is fed the value that each cell will take, since some have a preference to take value '0', others value '1'. This information can be used to generate a digital identifier (ID) number.



(a) (b)

Fig. 1.1 (a) SRAM cell logic circuit and (b) SRAM cell electrical circuit in CMOS technology.

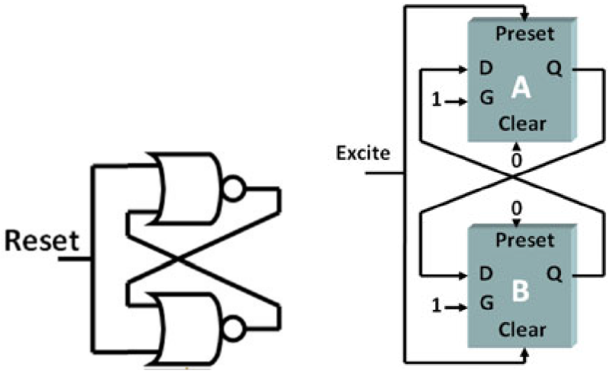
2. **"Butterfly" PUFs cells**: This type of cells have been tested in FPGAs. The type of cell used is shown in the Figure 1.2(b). These cells can be returned to a state of unstability using the preset and clear signals, which is perfectly comparable to the unstability after being powered up.

3. **Latch PUFs**: A latch PUF is very similar to SRAM PUFs. The difference is that the latch uses two cross-coupled NORs instead of two inverters. After receiving a reset signal, the latch becomes unstable as it happens with the SRAM memory cells. A diagram of the logical circuit is shown in the Figure 1.2(a).

4. **Flip-flops PUFs**: They are equivalent to PUFs with SRAM, but using flip-flops.

1.3 Scenarios for the application of PUFs

In this section we will summarize the different applications of the PUFs, which are fundamentally: system identification (explained in Section 1.3.1) and secret key generation (Section 1.3.2).



(a) (b)

Fig. 1.2 (a) Logic circuit of a latch and (b) schematic of a PUF cell “butterfly”.

1.3.1 Identification of systems

Due to the unclonability property, using PUFs for identification is very interesting for anti-counterfeiting technology. The PUF response can be used directly for identification in a manner very similar to a biometric identification scheme.

During an “enrollment” phase, a series of information of all the PUFs of the population are stored in a database, together with the identity of the PUF integrated in the system. During the identification, the identifier chooses a random challenge and requests a response to the PUF. If the response is sufficiently close to the correct one, the system is identified, otherwise an error occurs. In order to avoid repetition attacks, each stored information must be removed from the identifier after identification and used only once. The threshold to accept an identification depends on the distance between the Intra Hamming distance and the Inter Hamming distance. If both histograms do not overlap, the identification can be made by setting a threshold at an intermediate point between them. If they overlap, you have to establish limits to meet a compromise between the false acceptance rate (FAR) and the false rejection rate (FRR). The choice of the optimal decision threshold for the FAR and the FRR is shown in the Figure 1.3. Other types of thresholds may be desirable according to the purpose of application (for example, a threshold that ensures a false null rejection or a false null acceptance).

1.3.2 Secret key generation

PUFs intrinsic to integrated circuits have interesting properties for secret key generation and storage. Since the key is generated from an intrinsic randomness introduced by unavoidable

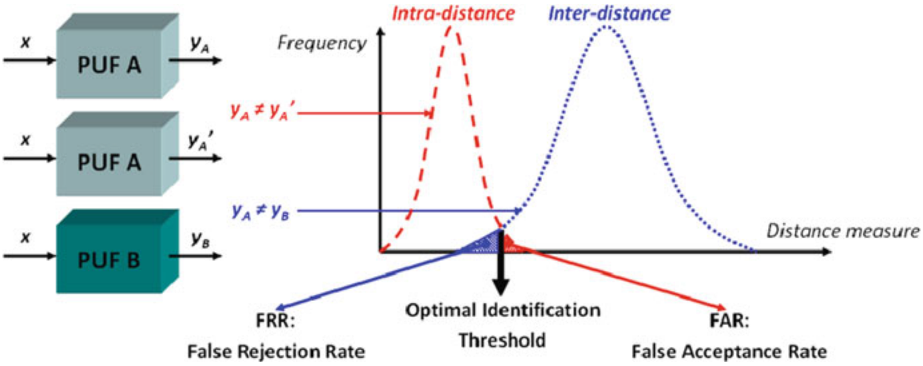


Fig. 1.3 Choosing the optimal threshold for FAR and FRR

manufacturing variations, an explicit programming step of the key is not necessary, which simplifies its distribution. On the other hand, since this randomness is fixed permanently in the physical (sub-) microscopic details, a non-volatile memory is not necessary for the storage of the key. This also offers additional security against attacks, invasive and semi-invasive attacks, since the key is not stored in digital format, but only stored in volatile memories when it is required to perform operations. In addition, the evidence of manipulation of the PUFs can be used to provide counterfeit-proof key storage.

Uniform randomness and reliable keys are necessary for cryptographic algorithms. If the responses of the PUFs are noisy and contain a limited amount of entropy, they can not be used directly as keys. An intermediate processing is necessary to extract the key from the response. This problem is known in information theory as the extraction of nearby secrets and is usually solved by a two-phase algorithm. During the initial phase of *generation*, the PUF is queried and the algorithm provides a secret key along with some additional information usually called *helper data*. In the *reproduction* phase, the verifier delivers the *helper data* to the algorithm that uses it to extract the same key from the PUF as in the *generation* phase. In this way, the device contains the PUF and the verifier has a stable secret key. It is possible to build these algorithms in such a way that the key is completely secret, even if the *helper data* is observed, for example, in the case that the *helper data* is publicly communicated from the verifier to the device. Instances of these algorithms have been proposed in [5] and the cost of implementing them is discussed in [6, 7].

1.4 Use of SRAMs as PUFs

SRAM PUFs, which were introduced in [8], and are based on feedback circuits (see Figure 1.4) that have two stable states of operation and one unstable. If the circuit is at the unstable state, the slight differences between the two symmetrical parts make it tend to a stable state. This means that every time the cell is powered, it will give the output value '0' or '1' depending on the relative differences between the inverters. Therefore, the output value of each memory element depends on variations in the manufacturing process and the noise that may affect the element.

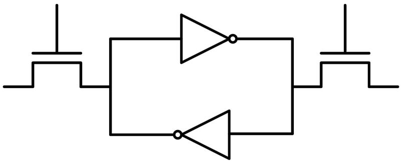


Fig. 1.4 Basic structure of a SRAM cell

The ID obtained from the SRAM PUFs is formed by the concatenation of the output values of different memory locations, ideally, forming a single random sequence. Therefore, the challenges of SRAM PUFs are the memory positions that generate the response. It is also necessary that the PUFs used for IDs or generation of secret keys comply with certain statistical characteristics in order to ensure uniqueness (for security) and repeatability (for reliability).

The viability of the SRAM PUFs depends on the sensitivity of the memory cells to the environment, where the circuit will be used at certain values of temperature and supply voltage. The PUF internal characteristics are basically defined by variations in the manufacturing process, but may vary due to stress conditions or aging. Under certain circumstances, some especially sensitive cells can provide different initialization values from one experiment to another when they are excited with the same challenge (in the same memory locations). This is known as a "bit flipping" effect [9, 10]. This effect is decisive for the behavior of the PUF and clearly decreases the uniqueness and reliability.

In order to characterize the SRAM PUFs completely, and therefore, to analyze the possible impact on the structure of these effects it is important to understand the basic principles of the constituent elements, which usually consist of two crossed inverters and two other access transistors. A typical SRAM 6-T CMOS structure is shown in the Figure 1.5.

Ideally, the manufacturer would like to be able to implement the two inverters of the SRAM cell as identical as possible, since this improves the power and speed characteristics of the memory [3]. However, in reality, due to variations in the manufacturing process, there

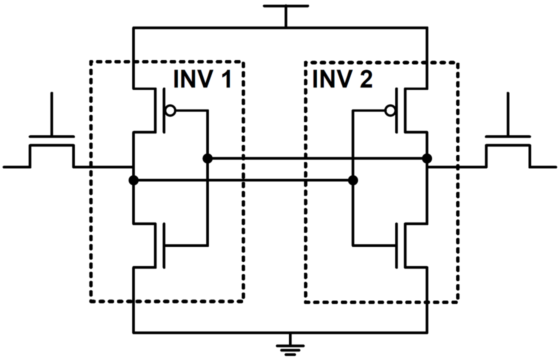


Fig. 1.5 Internal structure typical of a SRAM 6-T CMOS cell

are small differences (or “mismatching”) in the cells, which means that the inverters will not have exactly the same behavior. In practice, SRAM cells are built with the appropriate width and length dimensions between different transistors [11], in such a way that these fluctuations do not affect reading or writing in a habitual way. However, during start-up, inverters are not subject to any external input signal. On the other hand, any minimum voltage difference will cause one of the two to start conducting before the other. This will cause the cell to be displaced toward ‘0’ or toward ‘1’ due to the amplifying effect produced by the feedback of the output of each inverter with the input of the other. Holcomb and Cortez in [12, 13], already divide the cells depending on their Voltage Transfer Curve (VTC), between those that have a high displacement (“asymmetric cells”) and therefore a greater probability of evolving to a stable state (‘0’ or ‘1’), and those that do not have a strong tendency toward any state and start with any state, either ‘0’ or ‘1’ (“neutral cells”). Figure 1.6 shows a neutral cell not displaced and a cell completely displaced in VTC for both elements.

Due to the characteristics of the SRAM PUFs, and like any memory structure, they are susceptible to aging that can deteriorate in a different way the threshold voltage of the transistors, channel length, etc. causing an initially neutral cell to exhibit some displacement. Guajardo in [8] estudied this effect on the start-up of SRAMs integrated in Xilinx devices, by simulating the use of a normal memory by writing ‘0s’ and ‘1s’ and maintaining the state of memory around 10 minutes per every writing. The results obtained on the SRAM restart values, showed that this affects in a very small way the initial value of the SRAM (less than a 5% variation). Holcomb in [13] also analyzes the influence of Negative Bias Temperature Instability (“NBTI”) on start-up values. The NBTI study consists in modifying the threshold voltage (V_{Th}) of the MOS transistor over time due to stress conditions applied by temperature changes. This effect has more influence on PMOS transistors than on NMOS [14]. After

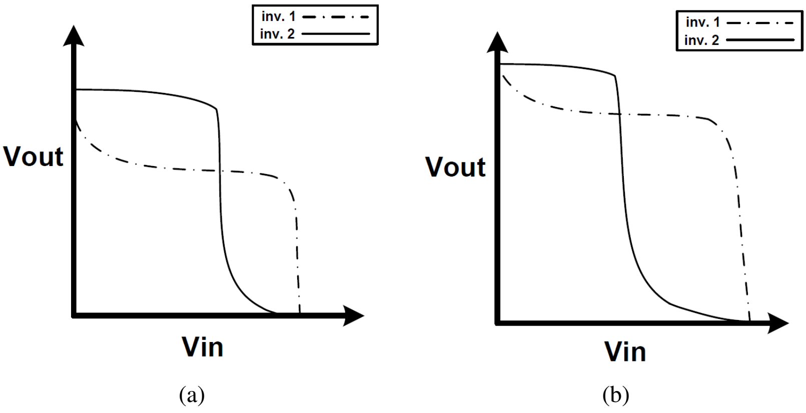
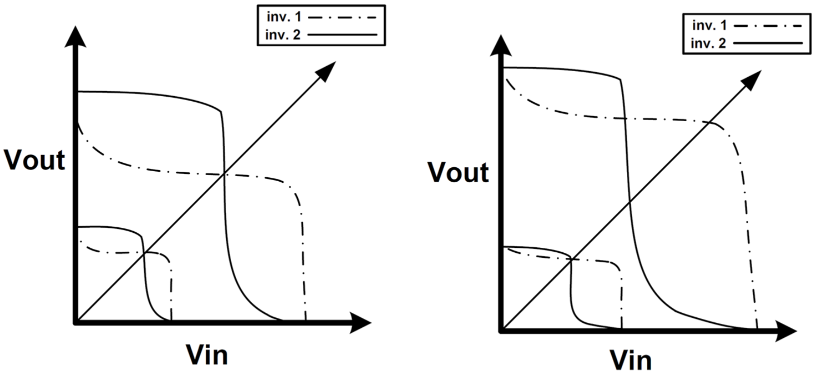


Fig. 1.6 (a) VTC for neutral cell and (b) VTC for asymmetric cell.

the stress situation ceases, the devices begin to recover. If used in a normal manner, the devices operating intermittently at low temperatures, NBTI should not be of concern as most cells can recover their neutral state. However, if the state of high temperature remains, the recovery is not fully realized, so the cells remain asymmetric permanently because of this effect, as in the case of aging or asymmetry due to the manufacturing process. The effect of temperature on CMOS is well studied in the literature, as well as its threshold voltage (V_{Th}) and the electron-hole mobility (μ) both dependent on the increase in thermal noise. The temperature thus influences the inclination of the VTC curves of the cells and therefore their final value. Nevertheless, as already presented in [13], those parameters that counteract this effect, such as the threshold voltage or mobility, have the same dependence on temperature but the opposite impact due to the sub-threshold current. This effect, together with the increase in the noise present with the temperature, makes the SRAM start-up values difficult to model. In addition, the influence of each MOS transistor in the start-up value of an SRAM cell is difficult to model since they are cross-coupled. Therefore, the only way to characterize SRAM is to measure the probability of a cell to be initialized at a certain value. There is a difference between the impact of temperature variation on the displacement of the cell and the mismatch, aging or NBTI, which is that the temperature does not permanently affect the displacement as do the other parameters. Therefore, a high increase in temperature can convert an asymmetric cell into a neutral or vice versa, but as soon as the temperature is restored, the cell will behave as initially did due to the other parameters.

Compared to the previous effects, the variations in the power supply do not affect the displacement of the cells, but they influence the "Static Noise Margin" (SNM) of the cells that quantifies the immunity of the SRAM cells against noise. The SNM of a given cell at a supply voltage is defined by the maximum voltage noise that can be reached before changing state [15]. It is defined as the shortest side of the largest box that can be placed inside the eye of the voltage transfer curves (VTC) of the cross inverters that make up the cell. As the power supply voltage values decreases, so does the eye of the VTC and in turn the immunity to noise, as shown in the Figure 1.7. In cells that are not displaced, low power supply voltage causes the SNM of each state to be equally small making them very sensitive to the effects of noise, while cells with a high tendency to a state, low power supply voltage can reduce the SNM of one state to zero by indicating that there is only noise in one of the two states.



(a)

(b)

Fig. 1.7 (a) Decrease in SNM with power supply voltage for a neutral cell and (b) for an asymmetric cell.

As described, the start-up values are highly dependent on the temperature and the supply voltage due to the influence on the VTC curves, the electron-hole mobilities, etc. Therefore, a good characterization of the impact of these effects is necessary to determine, not only the validity of the elements for use in authentication systems but also to provide a solution that eliminates or at least reduces these effects. In order to solve this problem, various approaches have been proposed, such as including additional information, post-processing, etc.

1.5 Use of SRAMs as TRNGs

The true random number generators (TRNGs) based on metastability are usually based on the cross-coupled elements, which show two different results determined basically by the manufacturing process and external noise. These elements interact with the position of the metastability point and therefore displace the final point of stability of the structure. They are in the first instance comparable to the RO TRNG, although they are gaining great interest in modern digital integrated circuits due to the advantages they bring for the simplicity of implementation, since they provide at the same time the extraction of entropy and digitization.

The first notions of TRNGs based on metastable elements are described in [16, 17], where a binary random number generator consisting of cascaded CMOS R-S latches was proposed. In this structure, the first latch generates a metastable state in itself and reads its final state in the second. In order to provide greater robustness against failures and allow for easier implementation, the *n* bit TRNG proposed in [18] has a structure that combines the basic mode of operation of a typical LFSR by changing the basic type D cells of the flip-flop by the 1-bit random number generators described in [16, 17]. This approach is based on the high symmetry restrictions of the latches used, and the weights of both latches apart from the need to force them exactly to the point of instability.

The results in [19], pointed out that it was not enough to rely solely on the symmetry of the design and suggest that it was necessary to keep the flip-flop initially at the metastable point to get a low offset. In addition to this, the structure must ensure that the variations in the displacement are much less than some voltage noise (value that would depend on the technology and the manufacturer) to obtain random bitstreams. The reason for this is to avoid that deterministic signals (like previous values of entrance of the flip-flop) can influence the output values, and thus produce a non-deterministic base element. For this purpose in [18], a structure based on the addition of a negative delay in the feedback loop of the second flip flop is proposed. Through the implementation of this structure the authors reduce drift and offset, and relax the strong restrictions on symmetric systems.

Later [20] introduced the concept of TRNGs based on metastability with quality control. The idea is to test the time of each metastable event. This would allow to determine the original noise level and therefore the randomness. In this way, the user can determine the compromise between the quality of the bitstream and the bit rate. Although statistically it has good quality values, this method requires a high cost in hardware. It is based on the time it takes for converters and digital controllers to extract statistical information for feedback and adjustment of latches. In addition to this, a memory is required to store the new calculated times if they are higher than a certain predefined threshold.

In this context, the elements based on SRAM appeared as a simple solution to provide low cost TRNGs with high quality properties. The main advantages of these structures compared to the previous approaches is that they do not require a special manufacturing process and are present in most of the existing digital designs. Therefore, as shown in the case of ID generation with these elements, the added advantage is the reuse of chip memory elements.

The first proposal to use SRAM elements as TRNG comes from Holcomb in [13]. The idea is to use the initial values of the SRAM as sources of entropy using privacy amplification techniques. However, only a part of the SRAM bits are noisy when they are powered and therefore the entropy of these bits needs to be condensed into a random seed of complete entropy. Basically, the conditioning algorithm is a compression function that compresses a certain amount of input data into smaller fixed-size bitstreams. The amount of compression required for the generation of a truly random output with complete entropy is determined by the minimum entropy of the input bits. The TRNG proposed by Holcomb in [13] presents a 128-bit TRNG obtained from a 512-byte SRAM memory block. The metric that is used to obtain minimum entropy values of 512-byte memory blocks is based on the probability of guessing. The value of each individual byte is obtained in the following way for 100 tests of each element:

$$\gamma(B_n) = maxP[B_n = b] : b \in \{0,1\}^8$$

Assuming that each bit is independent, the probability of guessing the 512-byte block is the product of the probability of guessing each byte:

$$\gamma(X) = \prod_{n=1}^{n=512} \gamma(B_n)$$

Being:

$$X = \{B_1, B_2, ..., B_{512}\}$$

The value of the minimum entropy provides an indicator of the amount of randomness. It is defined as follows:

$$H_\infty(X) = \log_2\left(\frac{1}{\gamma(X)}\right)$$

To obtain a 128-bit sequence of the 512 bytes of memory and thus amplify the obtained entropy, they used a PH hash function. The total area required, when both the SRAM and the hash PH function are included are 19.700 μm^2 that, compared to Tokunaga's proposal at [20] of 35.900 μm^2 accounts for almost half of the area. In addition, the Holcomb proposal does not require any precise control of any element like the previous approaches, which saves a lot of area and power consumption, even when the memory cells are not being used by another element of the system. If the SRAM is already included in the proposed system, it would only require the PH hash, which occupies only 7400 μm^2. However, the disadvantage of this approach is that the TRNG only generates entropy during the start-up. Therefore, if random numbers are needed at a time other than the start, it must be stored from start-up to use with the consequent safety problems. Therefore, it is indicated for applications that are fed intermittently and do not require large numbers of random numbers.

The work in [21] takes a step forward in the use of SRAM PUFs for TRNG in order to overcome these problems. Based on the ideas of Holcomb, they proposed the construction of a random number generator based on the mixture of a random deterministic bit generator (DRBG) with the start values of the SRAM, which provides a completely random seed. Therefore, the structure has advantages of both, such as generating high bit rates, thanks to the DRBG without the need to restart the SRAM every time a number must be generated, and the advantage of good statistical properties due to the truly random seed provided. by the start values of the SRAM. Van der Leest's scheme is shown in the Figure 1.8. The components used are:

- An SRAM memory connected to a conditioning algorithm to convert the SRAM start-up values into a truly random seed. In this case, the conditioning algorithm is responsible for compressing the bits of the memory into a random seed of complete entropy.
- A deterministic random number generator (DRBG) according to the specifications of the NIST 800-90 [22].

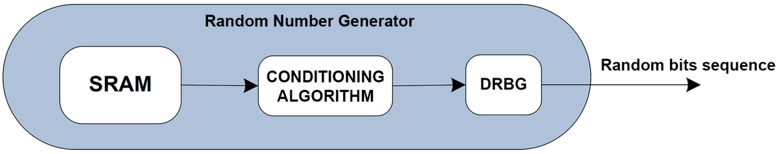


Fig. 1.8 Use of SRAM for random number generation.

The method used by Vincent Van der Leest [21] to define the value of the minimum entropy of a sequence of n bits is:

$$(H_{min})_{total} = -\sum_{i=1}^{n} \log_2(p_{i_{max}})$$

Where $p_{i_{max}}$ is the maximum of the probabilities presented by a cell i of taking a '0' or a '1'.

The measurements were made in 130 UMC SRAMs at different temperatures and different memory instantiations, concluding that the value of the minimum entropy can be obtained with 100 measurements. In addition, in these circumstances both Holcomb and Van der Leest have analyzed Cypress memories of 2KB at 150nm and 65nm, for which they obtained a minimum entropy of 2%. From these results they conclude that 1600 bytes are necessary to obtain a truly random 256-bit seed.

Based on these values they implemented the proposed structure in memories with 2.5% minimal entropy and 2KB SRAM. As a conditioning algorithm they used an SHA-256 function. Its output provides the necessary amount of bits for the DRBG. In these circumstances, the randomness obtained by the seed after the conditioning algorithm (SHA-256 hash) successfully passes all NIST randomization tests. The time required to acquire the seed is around $10.24\mu s$ when the circuit works at a clock frequency of 200MHz. The total area required is 55,000 equivalent gates, of which 25K corresponds to 2KB of memory, another 20K to SHA-256 and the remaining 10K to DRBG. The main advantage is that it is not necessary to regenerate the seed in a long period of time.

1.6 Conclusions

Physical Unclonable Functions have attracted a great interest throughout these years due to property of uniqueness. The group of memory-based intrinsic PUFs is of special interest because they are already part of almost any electronic product as volatile memories. Moreover, the entropy of PUF responses can be used for many purposes, among which are the generation of identifiers, secret keys, and true random numbers.

To analyze the memory-based PUFs in more detail and optimize them, the following chapter presents a method to simultaneously improve the quality of the identifiers, secret keys, and random numbers that can be generated from the start-up values of standard SRAMs. The method is based on classifying memory cells after evaluating their start-up values at multiple measurements in a registration phase. The registration can be done without unplugging the device from its application context, and with no need for a complex laboratory setup.

Chapter 2

Identifiers, secret keys, and random numbers from SRAMs

2.1 Summary

This Chapter presents a method to simultaneously improve the quality of the identifiers, secret keys, and random numbers that can be generated from the start-up values of standard static random access memories (SRAMs). The method is based on classifying memory cells after evaluating their start-up values at multiple measurements in a registration phase. The registration can be done without unplugging the device from its application context, and with no need for a complex laboratory setup. The method has been validated experimentally with standard low-power SRAM modules in two different appli- cation specific integrated circuits (ASICs) fabricated with the 90-nm TSMC technology. The results show that with a simple registration the length of the identifiers can be reduced by 45%, the worst case bit error probability (which defines the complexity of the error correcting code needed to recover a secret key) can be reduced by 64%, and the worst case minimum entropy value is improved, thus reducing the number of bits that have to be processed to obtain full entropy by 81%. The method can be applied to standard digital designs by controlling the external power supply to the SRAM using software or by incorporating simple circuitry in the design. In the latter case,

The content of this Chapter was published as *"Improved Generation of Identifiers, Secret Keys, and Random Numbers From SRAMs"* in the IEEE Transactions on Information Forensics and Security on December 2015, with DOI: 10.1109/TIFS.2015.2471279.

a module for implementing the method in an ASIC designed in the 90-nm TSMC technology occupies an active area of 42,025 μm^2.

Chapter 3

Design of a VLSI module based on SRAM PUFs to authenticate things

3.1 Summary

The algorithm proposed in Chapter 2 is lightweight enough to be carried out as a module and implemented in a VLSI system. Throughout this Chapter, details about the hardware implementation of this module have been shown, including its operating modes and architecture. The control block of the module was explained in detail, since it is in charge of the management of the other blocks, such as the read and write of a SRAM acting as a PUF.

With this module, it is possible to guarantee that a unique circuit generates the information sent and that the integrity of that information is not compromised. For that purpose, the

Part of the content of this Chapter was patented as *"Method and device for generating truly random numbers and identifiers"* on July 2016, with patent number ES2548792 B1.

An FPGA demo of prototype presented in Subsection 3.5 was published as *"Robust unclonable identifiers and true random numbers from off-the-shelf SRAMs"* in the Proceedings of the 2014 Conference on Design and Architectures for Signal and Image Processing (DASIP) on June 2015, with DOI: 10.1109/DASIP.2014.7115613.

A detailed version of the VLSI design presented in Subsection 3.6 was published as *"A VLSI module to authenticate unclonable things"* in the 2015 International Symposium on Consumer Electronics (ISCE) on June 2015, with DOI: 10.1109/ISCE.2015.7177831. Adapted versions of this design were published as *"CMOS digital design of a trusted virtual sensor"* in the IEEE Nordic Circuits and Systems Conference (NORCAS): NORCHIP and International Symposium of System-on-Chip (SoC) on October 2017, with DOI: 10.1109/NORCHIP.2017.8124948, and as *"VLSI Design of Trusted Virtual Sensors"* in Sensors Journal on January 2018, with DOI: 10.3390/s18020347.

module can be used to reconstruct de key and to generate the nonces required by an authentication protocol. This has been illustrated with a lightweight protocol based on symmetric cryptography. The following Chapter shows how the algorithm is so lightweight that it can be integrated not only in hardware but also in software in low-power and resources-constrained IoT devices.

Chapter 4

SRAM PUF-based software solutions to increase security of Bluetooth IoT devices

4.1 Summary

The use of SRAM start-up values to reconstruct the secret shared keys between different IoT devices adds another security layer to current systems, such as key fobs and smart locks, sensors nodes, or connected cameras. The use of PUFs inside the BLE hardware of IoT devices improves the security of firmware updates because the devices can be uniquely identified at low cost. In particular, using the entropy generated by their SRAM, the devices

Part of the content of this Chapter was published as *"Physical unclonable keys for smart lock systems using Bluetooth Low Energy"* on October 2016, with DOI: 10.1109/IECON.2016.7792955, as a complete version of the smart locks example presented in Subsection 4.3.6.

A detailed version of the nodes example presented in Subsection 4.3.6 was published as *"A PUF- and Biometric-Based Lightweight Hardware Solution to Increase Security at Sensor Nodes"* in Sensors Journal on July 2018, with DOI: 10.3390/s18082429.

A detailed version of the camera example presented in Subsection 4.3.6 was published as *"Trusted Cameras on Mobile Devices Based on SRAM Physically Unclonable Functions"* in Sensors Journal on October 2018, with DOI: 10.3390/s18103352, and as *"Using Physical Unclonable Functions for Internet-of-Thing Security Cameras"* in the SaSeIoT 2017: Interoperability, Safety and Security in IoT Conference on July 2018, with DOI: 10.1007/978-3-319-93797-7_16.

A detailed version of the protocol presented in Section 4.4 was published as *"Trustworthy firmware update for Internet-of-Thing Devices using physical unclonable functions"* in the 2017 Global Internet of Things Summit (GIoTS on August 2017, with DOI: 10.1109/GIOTS.2017.8016282.

can store all the secret keys obfuscated instead of in clear, and they can derive new fresh keys from the previous ones. Besides, since SRAMs are available in BLE chips, security is increased with no additional cost in hardware.

A registration process is required to generate the public data that are stored in the non-volatile memory of the physical key. In the case of key fobs based on the CC2541 BLE system on chip from Texas Instruments, a firmware was developed to reconstruct the secret key using the mask and helper/debiasing data and a repetition decoder without previous information about the secret key. The firmware was tested successfully in real scenarios that contain a CC2541 SoC and connected devices. Experimental results with BLE chips of IoT devices confirm that the obfuscated data do not reveal sensitive information and that the keys needed by the proposed algorithms are successfully reconstructed by only the original device. In addition, the nonces generated by the SRAM device are adequate to be used in Key Derivation Functions according to NIST. These results show how the security in BLE devices can be improved without any hardware modification but exploiting the existing hardware in the BLE chips. This opens the way to many other interesting security applications in industrial control systems and factory automation.

After demonstrating the integration possibilities in simple protocols for applications such as the secure firmware update, the next natural step is to think about integrating PUFs into cryptographically secure protocols. Therefore, throughout the next Chapter, the integration and implementation of a zero-knowledge protocol in a microcontroller will be developed, making use of the algorithm for extracting PUFs widely studied in previous Chapters. This new design will allow having a completely closed system, which is connected to the physical identity of the device and which in turn cryptographically guarantees the integrity and anonymity of the device's identity.

Chapter 5

PUF-derived IoT identities in a zero-knowledge protocol for blockchain

5.1 Summary and future work

We have described a novel anti-counterfeiting approach for IoT devices exploiting unique characteristics of memory chips for deriving a cryptographic secret combined with a blockchain for trusted and reliable verification of device identities. We have evaluated the approach with a microcontroller from Texas Instruments under different operating conditions. The results demonstrate the robustness of the approach in a wide range of temperatures, reducing the noise in the PUF responses by up to 90% compared to unprocessed responses. These results together with the implementation of the ZK-proof protocol go beyond related work by [23] in that the secret key is never known by the manufacturer and never leaves the device, facilitating both the authentication and the traceability of products by third parties.

We see a number of areas for future work. First, the results obtained for the Texas Instruments microcontroller need to be reproduced with a variety of memory types and

The content of this Chapter was published as *"PUF-derived IoT identities in a zero-knowledge protocol for blockchain"* in the Elsevier Internet of Things Journal on May 2019, with DOI: 10.1016/j.iot.2019.100057.

A summary of the content of this Chapter was published in a joint colaboration paper called *"Crypto anchors"* in the IBM Journal of Research & Development on February 2019, with DOI: 10.1147/JRD.2019.2900651.

microcontrollers. It would be important to pick configurations that are expected to be used in IoT deployments. For instance, wearable electronics and automation use cases are emerging in the coming years – many of them related to safety-critical functions that require protection from counterfeiting.

A second area for future work is to increase the accuracy and robustness of the fuzzy extractor, particularly under varying operating conditions, as well as implementing a computational fuzzy extractor. We have already investigated the influence of temperature. The impact of other operating conditions in empirical investigations needs to be understood. In this context, a framework and best practice to handle false-positive and false-negative identifications should be developed.

A third area is to investigate possible attack vectors and develop a threat model for attacking the approach. This model would include deliberately making a device not identify correctly, either in a denial-of-service attack or for staying unnoticed, as well as making a cloned device identify as an original device. Such attacks can be extended from identification into monitoring and control functions. On the other hand, more invasive attacks such as DPA should be considered which depend very much on the particular implementation.

Moreover, during the next Chapter, a new type of PUF will be presented that could be integrated into the zero-knowledge protocol explored throughout this Chapter. The integration between the PUF that will be proposed and the design described above will not be carried out in this Thesis, but it is also recommended as future work.

Chapter 6

Behavioral and Physical Unclonable Functions (BPUFs): SRAM example

6.1 Summary

The BPUFs proposed in this Chapter are tamper resistant, and tamper-evident to the physical attacks reported to current PUFs because those attacks change the behavioral responses of the BPUFs. Physical clones of BPUFs are more challenging to obtain since behavioral responses evaluate dynamic features. Experimental results with SRAM BPUFs show that the highest probability of an attacker to succeed in mathematically cloning the behavioral responses is as low as $1.5 \cdot 10^{-34}$.

While Hamming distance is employed to measure the similarity of current PUF responses, this Chapter shows that Jaccard distance is more suitable for evaluating behavioral responses. While the values of the bits are employed to measure the unpredictability of current PUF responses, this Chapter shows that binary-coded positions of the bits are more suitable for evaluating behavioral responses.

The content of this Chapter has been patented as “A behavioral and physical unclonable function and a multi-modal cryptographic authentication method using the same” on July 2019 with Application Number EP19382623.7, and submitted for publication as *“Behavioral and Physical Unclonable Functions (BPUFs): SRAM example”* to the IEEE Access Journal on July 2019.

The multimodal authentication protocol proposed is lightweight since it is based on symmetric cryptography. It obfuscates all the sensitive data (physical responses and cryptographic key with helper data algorithms and behavioral responses with salting techniques) and uses fresh data so that a non-protected communication channel can be employed between the BPUF instance and the verifier.

As an example of BPUFs, SRAM BPUFs have been presented and characterized experimentally using low-power dual-port 8-transistor SRAMs fabricated in 90-nm CMOS technology, considering nominal and non-nominal operating conditions (changing power supply voltage and temperature as well as aging the circuits).

Chapter 7

Final remarks

Throughout this thesis, SRAM PUFs have been analyzed, showing how not only variations in the manufacturing process affect their behavior but also the operating conditions of the circuit. In order to improve the response of the PUFs in Chapter 2, a classification algorithm has been proposed that selects the cells with a more stable behavior, as well as those that have a more unstable behavior. We have shown how the response of the stable cells selected by this algorithm can be used to generate identifiers or reconstruct secret keys, while unstable cells can be used to generate true random numbers.

We have also demonstrated how this selection algorithm can be integrated in VLSI hardware designs, as well as in the software of low-power Bluetooth enabled SoC in Chapters 3 and 4. This simplicity makes it ideal for integration into IoT devices, allowing to take advantage of the SRAM PUF of these simple circuits for adding a new security element.

In addition, given the improvement in the quality of the identifiers and secret keys generated, it has been shown how they can be introduced into secure protocols. Among them, in this thesis a secure firmware update protocol has been proposed, as well as an authentication based on zero knowledge proofs that use PUFs to generate the secret key of the protocol.

Finally, a new type of PUF that we have called BPUF has been proposed based on the dynamic behavior of SRAM cells. This new type of PUF presents, unlike traditional PUFs, the property of liveness, and it showed behavior that has required defining new metrics and analysis methods.

7.1 Future work

The integration of the BPUF proposed into the protocol of Chapter 5 has not been studied yet. Given the low Hamming distance of the BPUFs, it is considered that they would be an interesting element to use in the LPN alternative (instead of the xLPN version) proposed in the original paper of the implemented protocol. In this way, the binomial distribution of low weight could be generated naturally (instead of created by a pseudorandom number generator) and combined with the generation of the uniform distribution produced by the traditional PUF. This study is left as a proposal for future exploration.

On the other hand, outside the scope of this thesis, experiments have also been performed with a true random number generator based on ring oscillators. This type of random number generator also takes advantage of intrinsic randomness to the circuits to generate random sequences. By generating different oscillation frequencies depending on the delay introduced by each inverter that forms the ring oscillators, these types of circuits generate bits that meet the random requirements imposed by most standards. This TRNG will be analyzed in the future, and it includes a health test to evaluate the quality of the generated sequences, as well as a self-calibration to always position itself at the optimum point of operation.

Another future line to explore is the implementation of public key cryptography (elliptical curves or RSA) to make digital signatures that are easy to integrate into conventional protocols in combination with PUFs. This would allow generating identities for IoT devices that could, for example, sign transactions for blockchain with a low resource requirement. Other types of algorithms (ciphers or hashes) will also be contemplated for their simplicity and wide range of uses. In addition, continuing this line of research, IoT devices that use PUFs will be integrated in different types of blockchain in order to perform authentication and traceability of them in any application environment that requires guaranteeing the origin of the information.

References

[1] Ravikanth Pappu, Ben Recht, Jason Taylor, and Neil Gershenfeld. Physical one-way functions. *Science (New York, N.Y.)*, 297(5589):2026–30, sep 2002.

[2] Blaise Gassend, Dwaine Clarke, Marten van Dijk, and Srinivas Devadas. Silicon physical random functions. In *Proceedings of the 9th ACM conference on Computer and communications security - CCS '02*, page 148, New York, New York, USA, 2002. ACM Press.

[3] Roel Maes and Ingrid Verbauwhede. Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions. pages 3–37. 2010.

[4] Roel. Maes. *Physically unclonable functions : constructions, properties and applications*. Springer, 2013.

[5] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. pages 523–540. Springer, Berlin, Heidelberg, 2004.

[6] Julien Bringer, Hervé Chabanne, and Thomas Icart. On Physical Obfuscation of Cryptographic Algorithms. pages 88–103. 2009.

[7] Roel Maes, Pim Tuyls, and Ingrid Verbauwhede. Low-Overhead Implementation of a Soft Decision Helper Data Algorithm for SRAM PUFs. pages 332–347. 2009.

[8] Jorge Guajardo, Sandeep S. Kumar, Geert-Jan Schrijen, and Pim Tuyls. FPGA Intrinsic PUFs and Their Use for IP Protection. In *Cryptographic Hardware and Embedded Systems - CHES 2007*, pages 63–80. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.

[9] Mathias Claes, Vincent van der Leest, and An Braeken. Comparison of SRAM and FF PUF in 65nm Technology. pages 47–64. Springer, Berlin, Heidelberg, oct 2012.

[10] Georgios Selimis, Mario Konijnenburg, Maryam Ashouei, Jos Huisken, Harmke de Groot, Vincent van der Leest, Geert-Jan Schrijen, Marten van Hulst, and Pim Tuyls. Evaluation of 90nm 6T-SRAM as Physical Unclonable Function for secure key generation in wireless sensor nodes. In *2011 IEEE International Symposium of Circuits and Systems (ISCAS)*, pages 567–570. IEEE, may 2011.

[11] Franco Stellari, Peilin Song, Alan J. Weger, and Darrell L. Miles. Mapping systematic and random process variations using Light emission from Off-State Leakage. In *2009 IEEE International Reliability Physics Symposium*, pages 640–649. IEEE, 2009.

[12] Mafalda Cortez, Apurva Dargar, Said Hamdioui, and Geert-Jan Schrijen. Modeling SRAM start-up behavior for Physical Unclonable Functions. In *2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, pages 1–6. IEEE, oct 2012.

[13] D.E. Holcomb, W.P. Burleson, and K. Fu. Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers. *IEEE Transactions on Computers*, 58(9):1198–1210, sep 2009.

[14] M. Denais, V. Huard, C. Parthasarathy, G. Ribes, F. Perrier, N. Revil, and A. Bravaix. Interface Trap Generation and Hole Trapping Under NBTI and PBTI in Advanced CMOS Technology With a 2-nm Gate Oxide. *IEEE Transactions on Device and Materials Reliability*, 4(4):715–722, dec 2004.

[15] E. Seevinck, F.J. List, and J. Lohstroh. Static-noise margin analysis of MOS SRAM cells. *IEEE Journal of Solid-State Circuits*, 22(5):748–754, oct 1987.

[16] M.J. Bellido, A.J. Acosta, M. Valencia, A. Barriga, and J.L. Huertas. Simple binary random number generator. *Electronics Letters*, 28(7):617, 1992.

[17] M.J. Bellido, A.J. Acosta, M. Valencia, A. Barriga, and J.L. Huertas. A simple binary random number generator: new approaches for CMOS VLSI. In *[1992] Proceedings of the 35th Midwest Symposium on Circuits and Systems*, pages 127–129. IEEE.

[18] A J Acosta, M J Bellido, M Valencia, A Barriga, and J L Huertas. Fully Digital Redundant Random Number Generator in CMOS Technology. *ESSCIRC '93: Nineteenth European Solid-State Circuits Conference*, 1993.

[19] D.J. Kinniment and E.G. Chester. Design of an on-chip random number generator using metastability. In *Proceedings of the 28th European Solid-State Circuits Conference*, 2002.

[20] Carlos Tokunaga, David Blaauw, and Trevor Mudge. True Random Number Generator With a Metastability-Based Quality Control. *IEEE Journal of Solid-State Circuits*, 43(1):78–85, jan 2008.

[21] Vincent van der Leest, Erik van der Sluis, Geert-Jan Schrijen, Pim Tuyls, and Helena Handschuh. Efficient Implementation of True Random Number Generator Based on SRAM PUFs. pages 300–318. 2012.

[22] Elaine Barker and J Kelsey. Recommendation for random number generation using deterministic random bit generators (revised). 2007.

[23] Chenglu Jin, Charles Herder, Ling Ren, Phuong Nguyen, Benjamin Fuller, Srinivas Devadas, and Marten van Dijk. FPGA Implementation of a Cryptographically-Secure PUF Based on Learning Parity with Noise. *Cryptography*, 1(3):23, dec 2017.

MIGUEL A. PRADA DELGADO | CURRICULUM VITAE

Status:	Ph.D. candidate, Postdoctoral researcher at IBM
Fields:	Quantitative analysis, hardware security, blockchain
Languages:	Spanish (Native), English (C1)
Tech:	Matlab, Python, HDL, C/C++, Hyperledger, Ethereum, Go (Golang), Flutter (Dart), Java, Angular, JavaScript, Git

Summary

Result-oriented Ph.D. candidate with a strong knowledge of hardware security and microelectronics looking for new challenges in the field of blockchain technology.

Research experience

06/2019 - present **Postdoctoral resarcher** IBM Research (Zurich)

- Created an ownership transfer demo of IoT crypto-anchors in Hyperledger blockchain
- Developed the full stack demo. RESTful API, Go back end, Go chaincode, and Flutter UI

02/2019 - 05/2019 **Researcher on HARDBLOCK project** IMSE-CNM (Seville)

- Designed a scalable protocol to store certified measurements from IoT devices
- Created an architecture to reduce writing of data into Ethereum blockchain

12/2018 - 01/2019 **Researcher on HW-IDENTIoTY project** IMSE-CNM (Seville)

- Designed hardware solutions to manage identities in IoT ecosystems
- Implemented a wearable demo to generate user's digital identity in a trusted device

05/2018 - 08/2018 **Research intern** IBM Research (Zurich)

- Authenticated resource-constrained devices in Hyperledger using PUFs technology
- Implemented PUF-derived IoT identities in a zero-knowledge protocol for blockchain

09/2017 - 12/2017 **Visiting researcher** Harvard University (Boston)

- Used hardware fingerprints to securely manage blockchain-connected human identities
- Developed protocols to integrate HDL secure modules and SoCs into blockchain

01/2015 - 11/2018 **Researcher on ID-EO project** IMSE-CNM (Seville)

- Developed a counterfeit-resistant cryptographic system used for real-time video
- Designed an encrypted and authenticated protocol for constrained devices

10/2014 - 03/2017 **Researcher on SENIAC project** IMSE-CNM (Seville)

- Developed a C firmware that implements a key reconstruction algorithm for Bluetooth
- Improved BLE 4.1 spec. without modifying the standard. Supervised a young researcher

09/2013 - 09/2015 **Researcher on SEIs project** IMSE-CNM (Seville)

- Developed integrated IP-cores as technical researcher in the area of security
- Characterized and verified the modules in FPGAs and ASICs

09/2013 - 03/2015 **Researcher on CRIPTO-BIO project** IMSE-CNM (Seville)

- Developed a software/hardware FPGA demo that used PUFs to generate IDs and TRNs
- Characterized and modeled PUF's demo behavior under different operating conditions

Teaching experience

02/2018 - 05/2018 **Electric Circuits: Theory and Instrumentation** B.Sc. Physics (Seville)

- Taught 7 groups (with 15-20 students) of second year of Physics Bachelor Degree
- Supervised and evaluated students during laboratory lessons, homework and exams

09/2016 - 02/2017 **Digital Systems Design** B.Sc. Computer Science (Seville)

- Taught 1 group (with 10 students) of second year of Computer Science Bachelor Degree
- Supervised and evaluated students during laboratory lessons, homework and exams

02/2016 - 06/2016 **Electric Circuits: Theory and Instrumentation** B.Sc. Physics (Seville)

- Taught 7 groups (with 15-20 students) of second year of Physics Bachelor Degree
- Supervised and evaluated students during laboratory lessons, homework and exams

09/2015 - 02/2016 **Experimental Techniques I** B.Sc. Physics (Seville)

- Taught 5 groups (with 15-20 students) of fourth year of Physics Bachelor Degree
- Supervised and evaluated students during laboratory lessons, homework and exams

02/2018 - 06/2018 **Electric Circuits: Theory and Instrumentation** B.Sc. Physics (Seville)

- Taught 6 groups (with 20-25 students) of second year of Physics Bachelor Degree
- Supervised and evaluated students during laboratory lessons, homework and exams

Publications and patents

Balagurusamy et al.: Crypto anchors

V. S. K. Balagurusamy et al. "Crypto anchors". In: *IBM Journal of Research and Development* 63.2/3 (Mar. 2019), 4:1–4:12. ISSN: 0018-8646. DOI: 10.1147/JRD.2019.2900651.

Prada Delgado et al.: Behavioral and Physical Unclonable Functions (BPUFs): SRAM example

Miguel Angel Prada Delgado and Maria Iluminada Baturone Castillo. "Behavioral and Physical Unclonable Functions (BPUFs): SRAM example". In: *IEEE Access (Submitted for publication)* (2019).

Prada Delgado et al.: Patent: A behavioral and physical unclonable function and a multimodal cryptographic authentication method using the same

Miguel Angel Prada Delgado and Maria Iluminada Baturone Castillo. "Patent: A behavioral and physical unclonable function and a multimodal cryptographic authentication method using the same". In: *Application number EP19382623.7* (2019).

M. Á. Prada-Delgado et al.: PUF-derived IoT identities in a zero-knowledge protocol for blockchain

Miguel Ángel Prada-Delgado et al. "PUF-derived IoT identities in a zero-knowledge protocol for blockchain". In: *Internet of Things* (May 2019), p. 100057. ISSN: 2542-6605. DOI: 10.1016/J.IOT.2019.100057.

Arjona et al.: Using Physical Unclonable Functions for Internet-of-Thing Security Cameras

Rosario Arjona, Miguel A. Prada-Delgado, et al. "Using Physical Unclonable Functions for Internet-of-Thing Security Cameras". In: Springer, Cham, Nov. 2018, 144–153. Best paper award. DOI: 10.1007/978-3-319-93797-7_16.

Arjona et al.: Securing Minutia Cylinder Codes for Fingerprints through Physically Unclonable Functions: An Exploratory Study

Rosario Arjona, Miguel Angel Prada-Delgado, et al. "Securing Minutia Cylinder Codes for Fingerprints through Physically Unclonable Functions: An Exploratory Study". In: *2018 International Conference on Biometrics (ICB)*. IEEE, Feb. 2018, pp. 54–60. ISBN: 978-1-5386-4285-6. DOI: 10.1109/ICB2018.2018.00019.

Arjona et al.: A PUF- and Biometric-Based Lightweight Hardware Solution to Increase Security at Sensor Nodes

Rosario Arjona, Miguel Ángel Prada-Delgado, et al. "A PUF- and Biometric-Based Lightweight Hardware Solution to Increase Security at Sensor Nodes". In: *Sensors (Basel, Switzerland)* 18.8 (July 2018). ISSN: 1424-8220. DOI: 10.3390/s18082429.

Arjona et al.: Trusted Cameras on Mobile Devices Based on SRAM Physically Unclonable Functions

Rosario Arjona, Miguel A Prada-Delgado, et al. "Trusted Cameras on Mobile Devices Based on SRAM Physically Unclonable Functions". In: *Sensors (Basel, Switzerland)* 18.10 (Oct. 2018). ISSN: 1424-8220. DOI: 10.3390/s18103352.

Martínez-Rodríguez et al.: VLSI Design of Trusted Virtual Sensors

Macarena Martínez-Rodríguez et al. "VLSI Design of Trusted Virtual Sensors". In: *Sensors* 18.2 (Jan. 2018), p. 347. ISSN: 1424-8220. DOI: 10.3390/s18020347.

Martinez-Rodriguez et al.: CMOS digital design of a trusted virtual sensor

Macarena C. Martinez-Rodriguez et al. "CMOS digital design of a trusted virtual sensor". In: *2017 IEEE Nordic Circuits and Systems Conference (NORCAS): NORCHIP and International Symposium of System-on-Chip (SoC)*. IEEE, 2017, pp. 1–5. ISBN: 978-1-5386-2844-7. DOI: 10.1109/NORCHIP.2017.8124948.

M. A. Prada-Delgado et al.: Trustworthy firmware update for Internet-of-Thing Devices using physical unclonable functions

M. A. Prada-Delgado, A. Vazquez-Reyes, and I. Baturone. "Trustworthy firmware update for Internet-of-Thing Devices using physical unclonable functions". In: *2017 Global Internet of Things Summit (GIoTS)*. IEEE, June 2017, pp. 1–5. ISBN: 978-1-5090-5873-0. DOI: 10.1109/GIOTS.2017.8016282.

M. A. Prada-Delgado et al.: Physical unclonable keys for smart lock systems using Bluetooth Low Energy

M. A. Prada-Delgado, A. Vazquez-Reyes, and I. Baturone. "Physical unclonable keys for smart lock systems using Bluetooth Low Energy". In: *IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society*. IEEE, Oct. 2016, pp. 4808–4813. ISBN: 978-1-5090-3474-1. DOI: 10.1109/IECON.2016.7792955.

Miguel A. Prada-Delgado et al.: SRAM-based Physical Unclonable Keys for BLE Smart Lock Systems

Miguel A. Prada-Delgado, Alfredo Vazquez-Reyes, and Iluminada Baturone. "SRAM-based Physical Unclonable Keys for BLE Smart Lock Systems". In: *2016 DATE - Design, Automation & Test in Europe*. Dresden (Germany), 2016.

Iluminada Baturone et al.: A VLSI module to authenticate unclonable things

Iluminada Baturone, Miguel A. Prada-Delgado, and Susana Eiroa. "A VLSI module to authenticate unclonable things". In: *2015 International Symposium on Consumer Electronics (ISCE)*. IEEE, June 2015, pp. 1–2. ISBN: 978-1-4673-7365-4. DOI: 10.1109/ISCE.2015.7177831.

Iluminada Baturone et al.: Improved Generation of Identifiers, Secret Keys, and Random Numbers From SRAMs

Iluminada Baturone, Miguel A. Prada-Delgado, and Susana Eiroa. "Improved Generation of Identifiers, Secret Keys, and Random Numbers From SRAMs". In: *IEEE Transactions on Information Forensics and Security* 10.12 (Dec. 2015), pp. 2653–2668. ISSN: 1556-6013. DOI: 10.1109/TIFS.2015.2471279.

Prada Delgado et al.: Patent: Method and device for generating truly random numbers and identifiers

Miguel Angel Prada Delgado, Maria Iluminada Baturone Castillo, and Susana Eiroa Lorenzo. "Patent: Method and device for generating truly random numbers and identifiers". In: *Patent number ES2548792A1* (2014).

Miguel A. Prada-Delgado et al.: Robust unclonable identifiers and true random numbers from off-the-shelf SRAMs

Miguel A. Prada-Delgado, Susana Eiroa, and Iluminada Baturone. "Robust unclonable identifiers and true random numbers from off-the-shelf SRAMs". In: *Proceedings of the 2014 Conference on Design and Architectures for Signal and Image Processing*. IEEE, Oct. 2014, pp. 1–2. ISBN: 979-10-92279-06-1. DOI: 10.1109/DASIP.2014.7115613.

Education

12/2014 - present	**Ph.D. candidate in Micro/Nano Electronics**	University of Seville

- "Physical Sciences and Technologies" Doctoral Programme from the Faculty of Physics
- Thesis topic: "Hardware-software solutions for cyber-physical secure systems"

10/2013 - 10/2014 **M.Sc. in Micro/Nano Electronics** Faculty of Physics (Seville)

- Highest GPA Award from the University of Seville received in 10/2014
- Master Thesis: “Unclonable Identifiers and TRNG from Static Memory Cells”

09/2008 - 09/2013 **B.Sc + M.Sc. in Telecommunication Engineering** ETSI (Seville)

- 300 ECTS Degree. Subjects from CS, electronics, telematics, RF comm. and robotics
- Master Thesis: “Use of PUFs based on Static Memory Cells for Security Applications”

Awards and recognitions

09/2017 - 12/2017 **Research visit scholarship** Harvard University (Boston)

- Three months scholarship from the Real Colegio Complutense at Harvard University

06/2016 **Spinf-off public recognition** University of Seville

- Oclose Inc. was publicly recognized as Spin-off of the University of Seville

09/2014 - 09/2015 **1-year acceleration of Oclose Inc. from Telefonica** El Cubo (Seville)

- Oclose Inc. received one year of acceleration from Telefonica startup accelerator

06/2015 **Invited speaker in “Coffee with Science”** University of Seville

- Participated as speaker in “Coffee with Science” day in the University of Seville

12/2014 - 12/2018 **Ph.D. scholarship** University of Seville

- Received a four-year Ph.D. grant from the V Research Plan of the University of Seville

10/2014 **Highest GPA Award** University of Seville

- M.Sc. in “Microelectronics: Design and Applications of Micro/Nanoscale Systems”

06/2014 **Best business project. €10,000 award** University of Seville

- Winners of “IX Contest of Business Initiatives” contest against more than 200 projects

06/2014 **Best Master Thesis project. €500 award** University of Seville

- Winner of “IX Contest of Business Initiatives” contest of Master Thesis projects

Leadership and entrepreneurship

02/2016 - present **Co-organizer of Ethereum Meetup Group** La Colmena (Seville)

- Teach free seminars about blockchain and smart contracts programming
- Organize periodical meetings to work with cryptocurrency miners and testnets

09/2014 - 06/2018 **Co-founder and CEO** Oclose Inc. (Seville)

- Lead the team to design and manufacture secure IoT devices for our scalable network
- Accelerated by Telefonica. Got working MVP and multiple contracts with SME

11/2013 - 09/2014 **Project lead** Apenkey (Seville)

- Invented authenticated products using Physical Unclonable Functions as fingerprints
- Winners of US contest against more than 200 projects. Awarded with €10,000