This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2017.2702607, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

Implementation and characterization of a physical unclonable function for IoT: a case study with the TERO-PUF

Cédric Marchand*, Lilian Bossuet*, Ugo Mureddu*, Nathalie Bochard*, Abdelkarim Cherkaoui†, Viktor Fischer*
*Hubert Curien Laboratory
18 rue Prof. Lauras, St.-Etienne, France
Emails: (firstname.lastname)@univ-st-etienne.fr
†TIMA Laboratory
46, Avenue Felix Viallet, Grenoble, FRANCE
Email: abdelkarim.cherkaoui@imag.fr

***Abstract*—Today, life is becoming increasingly connected. From TVs to smartphones, including vehicles, buildings, and household appliances, everything is interconnected in what we call the "Internet of Things" (IoT). IoT is now part of our life and we have to deal with it. More than 10 billion devices are already connected and five times more are expected to be deployed in the next five years. While deployment and integration of IoT is expanding, one of the main challenge is to provide practical solutions to security, privacy and trust issues in IoT. Protection and security mechanisms need to include features such as interoperability and scalability but also traceability, authentication and access control while remaining lightweight. Among the most promising approaches to such security mechanisms, physical unclonable functions (PUF) provide a unique identifier for similar but different integrated circuits using some of their physical characteristics. These types of functions can thus be used to authenticate integrated circuits, provide traceability and access control. This paper presents a comprehensive case study of the transient effect ring oscillator (TERO) PUF from its implementation on FPGAs to its complete characterization. The implementation of the PUF is detailed for two different families of FPGAs: Xilinx Spartan 6 and Altera Cyclone V. All the metrics used for the characterization are explained in detail and the results of the characterization include robustness to environmental parameters including variations in temperature and voltage. Finally, we compare our results with those obtained for another PUF: the ring oscillator (RO) PUF. All the design files are available online to ensure repeatability and enable comparison of our contribution with other studies.**

***Index Terms*—Physical unclonable function, PUF design, FPGA, PUF characterization**

I. Introduction

The Internet of Things (IoT) is a structure of interconnected smart devices, mechanical and digital machines, objects, animals or people associated with unique identifiers that have the ability to communicate over a network without the need for human action. Among many examples one is the smart campus Bosch installed at the Carnegie Mellon University [1]. Today more than 10 billion devices are already connected and five times more devices are expected to be connected in the next few years. IoT is here to stay and we need to provide solutions to the existing issues it involves. This new environment in which every object is connected enhances the life experience of all users, but also presents several challenges related to security and privacy. These security challenges are among the main barriers to the massive deployment of IoT on a world scale [2], [3], [4]. Indeed cryptographic algorithms designed to secure large computer devices such as servers, desktops, tablets and smartphones cannot necessarily be scaled down to function effectively on the smaller devices that make up the IoT. Since the IoT enables the Internet to reach the real world of physical objects, security needs to operate at different levels including communication, authentication, access control and traceability [5], [6].

Indeed, the traceability of the hardware is one of the primary needs in the IoT. Unlike many other security issues, traceability is more specific to the IoT as it enables people have confidence in the devices used in many applications. For example, it makes it easier to provide traceability for everyday products such as food, and furniture [5]. But more important, in a system where billions of chips are interconnected, the traceability of each element of the system is absolutely essential. A single compromised chip in a sensor network that operates in a sensitive application (the transport of frozen food for example) can have disastrous consequences in terms of cost and potentially human lives. In addition, improving the traceability of devices in IoT will help provide evidence for forensic investigations among others.

Authentication and access control are among the most important features of the IoT that need to be implemented. Today, authentication schemes using secret keys stored in non-volatile memories are extremely vulnerable due to the development of active attacks such as probing [7], as well as passive attacks [8]. Protection against these types of attacks is very expensive and thus not suitable in the context of the IoT with its size and energy constraints. In addition, the IoT includes billions of heterogeneous devices, some of which

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2017.2702607, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

may be re-programmable. Thus, users may define policies and permissions for their own use, and protection mechanisms should provide interoperability, flexibility and scalability while remaining lightweight [9].

Physical unclonable functions (PUFs) are a promising way to ensure authentication, access control and traceability. PUFs provide secure and low-cost authentication [9], [4]. Many architectures have been proposed for PUFs in the related literature, and they can be divided into groups [10]. One of these groups includes memory based PUF such as the SRAM PUF [11] and the DRAM-PUF [12], [13]. Another group includes delay based PUF such as arbiter PUF [14], ring oscillator (RO) PUF [15], loop PUF [16] and RS latch PUF [17]. Many studies have shown that the RO-PUF is the best candidate for FPGAs (*eg.* [18], [19], [20], [21]). Unfortunately, the RO-PUF has a security problem: it can be cloned using electromagnetic analysis [22] or RO cells can be locked using electromagnetic injections [23]. The transient effect ring oscillator (TERO) PUF has been proposed to solve this problem [24]. The TERO-PUF is similar to the RO-PUF, but the TERO-PUF uses TERO cells that have two possible states: a transient oscillating state (characterized by the oscillating frequency of the cell output and by the number of oscillations before the stable state is reached) and a stable state (characterized by the logical value of the TERO cell output).

In this article, we propose a complete case study to build a PUF that can be used in the IoT: the TERO-PUF. The implementation of the TERO-PUF and its characterization are described for two different recent FPGA technologies: Xilinx Spartan 6 (45 nm CMOS) and Altera Cyclone V (28 nm CMOS). As the TERO-PUF has been evaluated for older technologies (ASIC 350 nm and FPGA Altera Cylcone II), it is an absolute nessecity to compare its results on recent technologies. Indeed, process variations change with every new technology and a PUF with good characteristics on old technologies might not have good characteristics on new technologies. In addition, it is needed to completely re-implement a PUF for every technology since the basic cells are changing. This task is technically difficult but necessary and successfully implement a PUF on new technologies prove its feasibility and reliability over the time.

The rest of the article is organized as follows: Section II presents the TERO cell and details its implementation in the two FPGA families. Section III describes the overall system used for characterization. Section IV presents the metrics and parameters used to characterize the TERO-PUF. Section V gives the results of characterization and compares them in the two technologies. TERO-PUF results are also compared with those obtained using an implementation of the TERO-PUF in ASIC and compared to another PUF: the RO-PUF. Section VI explains how and why it is possible to use the TERO-PUF in the IoT context. Finally, Section VII summarizes and concludes the paper.

II. The TERO cell and its designs

The implementation of the TERO cell requires symmetry in the data path delays. Unfortunately, it is very challenging to control the exact place and route tool for FPGA. Thus, a special flow needs to be followed and the TERO cells of the PUF need to be implemented at the lowest accessible level for each technology.

A. The TERO Cell

The TERO cell is a metastable structure that was first presented in [25]. The structure was originally used as a true random number generator but has the right characteristics to be used as a PUF [26], [24]. Figure 1 presents the generic structure of the TERO cell. The TERO cell is composed of two identical and symmetrical branches (Branch 1, Branch 2). Each branch is designed with an initialization stage (typically an And gate) and an odd number of inverters. The same number of inverters is used for the two branches of the TERO cell.

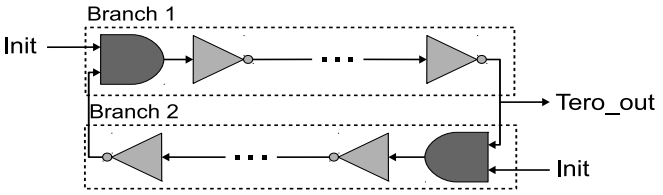

Figure 1. Generic Structure of a TERO cell

When the cell is initialized (rising edge of the signal "$init$"), two events begin to propagate inside the TERO cell and start oscillating. Depending on the mismatch in the delays between the two branches of the TERO cell caused by variations in the CMOS process, these two events move inside until they collide and stop the oscillating state. This behavior results in a finite number of oscillations of the TERO cell output ($TERO\_out$ in Figure 1). In theory, if all the gates and all the connections inside the TERO cell are perfectly identical, the cell would oscillate infinitely, but, due to variations in the manufacturing process, this case is extremely rare. The authors of [27] show that the number of transient oscillations increases with the number of inverters in each branch of the TERO cell. This structure was studied as a proof of concept for PUF design in [24]. Altera Cyclone II (90 nm CMOS) was used for this preliminary work.

To successfully implement the TERO cell in FPGAs, certain constraints need to be taken into account. First, the number of inverters has to be exactly the same in the two branches of the cell. Next, all connections between the different elements need to be pairwise equal. That means, for example, that the delay in connection between the initialization stage (And) and the first inverter needs to be the same in the two branches. Finally, the connections linking the two branches together also have to be equal in terms of delay. The first constraint appears to be quite easy to overcome because designers thinks they have complete control of the number of elements to be implemented but this is not really the case with Altera FPGAs (see Section II-C). In addition, the two last constraints are particularly challenging with all SRAM FPGAs. Indeed, control of the connections used by the place and route tool is not simple and only the placement of elements can be forced.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2017.2702607, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

Thus, finding a configuration that matches all constraints is not easy.

B. Design on Xilinx Spartan 6 FPGA

Xilinx Spartan 6 FPGAs (45 nm CMOS) are composed of an array of configurable logic blocks (CLB). Each CLB contains two elements called slices. There are three types of slices called slice_L, slice_M and slice_X. To implement the TERO cell inside the FPGA technology, only the same type of elements should be used, which is why only slices_X are used. This type of slice accounts for 50% of the FPGA, which makes it possible to implement many TERO cells. In addition, slices_X are the most simple slices inside Xilinx Spartan 6 FPGAs and contain only logical elements. Indeed, each slice_X contains four look up tables (LUT) with 6 inputs and 2 outputs. The two other types of slices (slice_M and slice_L) include other features such as memory LUTs and carry propagation logic. These features make it difficult to know exactly what is really inside the LUT. Thus, implementing the TERO cell using only slices_X makes the design more precise and better controlled. The TERO cell is designed using only basic components inside the FPGA, which is made possible by using the LUT6 component from the UNISIM library. This library is provided directly by Xilinx. In order to create any function using the LUT6 component, a 64-bit initialization vector has to be set as generic parameter. The value of this vector corresponds to the output according to the inputs used. More information about this component can be found in the Xilinx HDL library [28].

According to the properties of the TERO cells and to the structure of Xilinx Spartan 6 FPGA, the design needs to respect some additional constraints. First, a LUT must be used for one and only one gate. Then, it is necessary to use the minimum number of slices that allow the connections linking the two branches to have the same routing delay. Thus, the first choice is to use four slices to implement one TERO cell. Furthermore, using four slices allows the designer to create TERO cells with 1, 3, 5 or 7 inverters per branch. In order to choose the number of inverters used for the characterization of the TERO-PUF, the mean number of oscillations and the standard deviation of the number of oscillations have been recorded on Xilinx Spartan 6 FPGAs for different cell sizes (1, 3, 5 and 7 inverters per branches). Figure 2 presents the results of this evaluation.

Figure 2.a shows that the mean number of oscillations of the TERO cells increases linearly with the number of inverters. However, no conclusion can be drawn from the standard deviation of the number of oscillations (Figure 2.b). Indeed, the number of inverters per branch in the TERO cell does not have a significant impact on the standard deviation of the number of oscillations. Finally, to compare our TERO-PUF design with the study presented in [27], using 7 inverters per branch is appropriate. Seven elements are thus implemented per branch in this paper. Figure 33 is a schematic diagram of the TERO cell designed for Xilinx Spartan 6 FPGAs.

When the number of inverters on each branch of the TERO cell has been chosen, each element has to be positioned

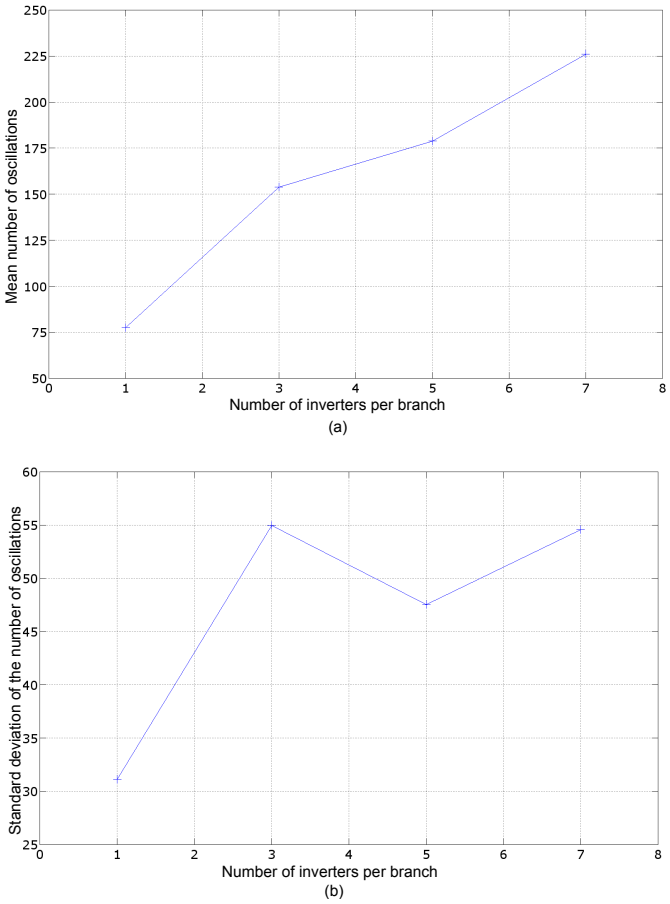

Figure 2. Evaluation of the mean number of oscillations and of the standard deviation of the number of oscillations according to the number of inverters per branch in the TERO cells

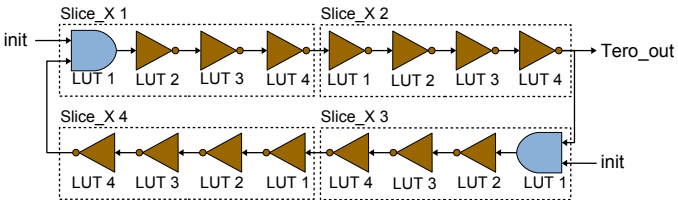

Figure 3. Schematic diagram of the TERO cell for Xilinx Spartan 6 FPGA with 7 inverters per branch

according to the diagram in Figure 3. This is achieved by forcing the placement of each element of the TERO cell in a user constraints file (ucf). To allow designers to reproduce the experimental results of this study, all design files are available online [29]. An estimation of the delays between each gates inside a TERO cell is provided by the Xilinx tool called "FPGA editor". According to this tool, all paths of the structure are pairwise identical (Table I), so all properties described in Section II-A are respected.

Finally, a hard macro (this is a feature of the Xilinx CAD tool that allows the designer to create pre-synthesized, pre-placed and pre-routed design blocks) is created to fix the routing of the TERO cell and to avoid any further modification from the synthesis tool. Indeed, a hard macro is an object which can be used as a component inside VHDL files and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2017.2702607, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

Table I
LENGTH OF TERO CELL CONNECTIONS ACCORDING TO XILINX TOOL (FPGA EDITOR)

From	To	Delay in branch 1 (ns)	Delay in branch 2 (ns)
AND	NOT_1	0.143	0.143
NOT_1	NOT_2	0.352	0.352
NOT_2	NOT_3	0.230	0.230
NOT_3	NOT_4	0.494	0.494
NOT_4	NOT_5	0.143	0.143
NOT_5	NOT_6	0.352	0.352
NOT_6	NOT_7	0.230	0.230
NOT_7	AND	0.626	0.626

more importantly, this component is never changed during optimization phases. The Xilinx tool for synthesis considers hard macros as black boxes that are simply replicated around one reference component placed in the user constraints file. The advantage of this method is that it is possible to copy and paste the TERO cell all over the FPGA. Furthermore, the Xilinx tool does not include additional logic inside hard macros. This ensures that the TERO cell is not altered by its insertion in the complete TERO-PUF system (see Section III).

C. Design on Altera Cyclone V FPGA

The structure of Altera Cyclone V FPGAs (28 nm CMOS) is completely different from that of Xilinx Spartan 6 FPGAs. Altera Cyclone V FPGAs are composed of an array of logic array blocks (LAB). Each LAB contains 10 adaptive logic modules (ALM) that each contain two LUTs with 6 inputs and 2 outputs. It is possible to implement LUT in VHDL files directly by using components from the altera_mf library. One component is LUT_input and represents one input of a LUT, the other is LUT_output and represents one output. To configure a LUT with a specific logical operation, this operation is directly applied to the LUT_input and LUT_output signals in the VHDL file.

Unfortunately, the Altera synthesis tool always optimizes logic function and merges some LUTs even when constraints are set. This means there is no advantage in using LUT directly in VHDL to implement the TERO cell in Altera FPGAs. To overcome this problem, there is a delay element called LCELL that is not optimized by the tool. In this way, the TERO cell design differs slightly from the Altera Cyclone V FPGAs shown in figure 1. Indeed, only one inverter per branch is used and delay elements are added between the And gate and the inverter as shown in figure 4.

To implement a TERO cell on Altera Cyclone V FPGA with the same configuration as the TERO cell on Xilinx Spartan 6 FPGA, the implemented TERO cell has two inverters, two And gates and 12 LCELLs. Once the TERO loop is designed in VHDL, it needs to be placed in such a way that all delays are pairwise equal. Our first idea when placing the cell was to try and use only one LAB. However, after testing all possible configurations of the TERO cell elements, there was still a non-negligible difference in the delays (more than 1 ns) of the two branches. Thus, two LABs need to be used. These two LABs can be placed side by side or one above the other. After testing possible placements using two LABs, the best configuration gives a total difference of 0.035 ns as estimated using the Altera Timequest analyzer tool. The selected configuration uses two LABs side by side with a particular arrangement of the TERO cell elements inside the two LABs.

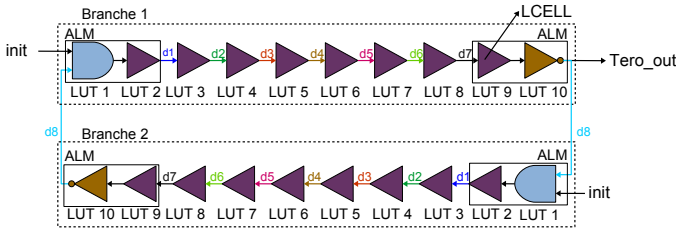

Figure 4. Schematic diagram of the TERO cell for Altera Cyclone V FPGAs with 6 delay elements (LCELL) and one inverter per branch.

Finally, to use the TERO cell to design the TERO-PUF (see Section III), each element of each TERO cell has to be placed in the Quartus setting file (qsf). In addition, to ensure that no logic is added by the tool during placement and route phases, a logic lock region including all TERO cells is created. Like in thecase of Xilinx Spartan 6 FPGAs, all design files are available online for the TERO-PUF design on Altera Cyclone V FPGA [29].

III. TERO-PUF SYSTEM

A. TERO-PUF architecture

To compare the two TERO-PUF designs with the two different FPGA technologies fairly, the same system has to be used. The system used in this article contains a hardware part and a software part. Figure 5 is a schematic of the system.

On the hardware side, two blocks of 128 TERO cells are implemented along with two 16-bit binary counters. To select one and only one TERO cell per block, two selectors are also implemented and two multiplexers are placed after the TERO cell blocks to drive the correct TERO output to the clock of the counters. Thus, when a challenge is sent to the device, only two TERO cells oscillate and their number of oscillations are returned by the FPGA.

On the software side, the number of oscillations received from the device under test are subtracted and the result is coded using the Gray code [27]. From this difference between the numbers of oscillations of two TERO cells, bits can be selected to build the PUF response finally analyzed.

One very important goal of this system is separating the TERO cells into two blocks because of security. Indeed, without this separation, first order dependencies appear inside generated signatures depending on which cells contribute to the response. Finally, it is possible to configure the time of acquisition, which corresponds to the time during which the TERO cells are able to oscillate.

Each block of TERO cells contains exactly 128 cells for this characterization. Thus, the number of possible challenges (pairs of TERO cells) is $128 * 128 = 16,384$ and the number of completely independent sets of 128 challenges is 128. It is possible to generate more signatures but they will have

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2017.2702607, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

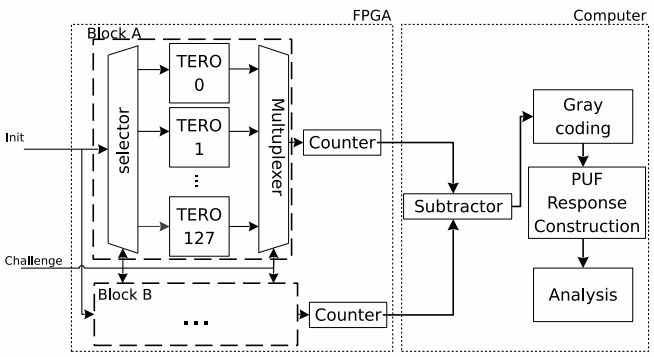

Figure 5. Hardware/software architecture of the TERO-PUF FPGA used for the characterization

some common subset of challenges. Considering that, the total number of all possible signatures corresponds to the number of bijections of a set itself.

B. Signatures generation

In order to build signatures of 128-bits using the TERO-PUF, it is needed to use multiples challenges/responses pairs. Indeed, the response to one challenge corresponds to some selected bits of the difference between the number of oscillations between the two selected TERO cells. Thus, it is not possible to extract 128-bits using only one challenge. The first step to generate complete signatures is to select which are the bits used as response of a challenge (see Section V-B). Using our PUF, it is possible to extract from one to three reliable bits of the difference between the number of oscillations of the two cells selected by the challenge. Then, it is possible to build signatures in many different ways but in this article, we choose to concatenate the responses obtained from the challenges sent to the TERO-PUF system. To illustrate the construction of one signature, let us consider that two bits are selected. These bits are considered as the response to a challenge c and are noted x_0x_1.

Let us note the first challenge sent to the system $c^{(1)}$, then the response to this challenge is the two bits noted $x_0^{(1)}x_1^{(1)}$. These bits are the two first bits of the signature $s = x_0^{(1)}x_1^{(1)}$. Then, we send another challenge $c^{(2)}$ and we add its response to the signature s we are building. Thus s becomes : $s = x_0^{(1)}x_1^{(1)}x_0^{(2)}x_1^{(2)}$. This process is repeated until the size of s reach 128. At the end, it is possible to remark that, in this example, s is the concatenation of the responses of the TERO-PUF to 64 challenges, so :

$$s = x_0^{(1)}x_1^{(1)}x_0^{(2)}x_1^{(2)} \ldots \ x_0^{(64)}x_1^{(64)}$$

In the rest of this paper, only signatures of 128 bits are considered, and if a signature is referenced as bit X, it means that the signature is built using this particular bit of the difference between the number of oscillations of the TERO cells. If the signature is referenced as bit X_1, X_2, it means that the signature is built using the two indicated bits per challenge, and so on. In order to select the bits of the PUF response that can be used to build signatures, the different configurations of construction have to be analyzed using different bits. This analysis is done using standard metrics and the parameters presented in the following section.

IV. Metrics and parameters for the characterization of the TERO-PUF

Before presenting the characterization results of the designed TERO-PUF, we now describe how the analysis is performed, what metrics are used, and identify the parameters involved in the characterization of the TERO-PUF.

A. Characterization metrics and randomness tests

The TERO-PUF is characterized using two principal metrics called uniqueness, steadiness (also known as reliability or stability), and randomness. With these three metrics, it is possible to evaluate the robustness of the PUF according to variations in temperature or voltage.

To stay within the scope of this article, let us consider a set of M FPGAs $(d_i)_{1\leq i\leq M}$, n-bit responses is extracted N times from the M FPGAs. The evaluation of the TERO-PUF is performed on 128-bit responses over 30 devices for Xilinx Spartan 6 and 18 devices for Altera Cyclone V ($n = 128$ and $M = 30$ or $M = 18$). The number of acquisitions used for the characterization is $N = 960$.

1) Uniqueness: Let us consider two devices d_i and d_k that give respectively responses r_i and r_k to the same challenge c. The probability that these two responses are different must be very high. Accordingly, uniqueness represents the variations in the responses of multiple chips to the same challenge and can be referenced as extra-chip variation (EC). To evaluate this metric, the following formula is used.

$$EC = \frac{1}{M(M-1)N}\sum_{i=1}^{M}\sum_{k=1,k\neq i}^{M}\sum_{j=1}^{N}\frac{HD(r_{i,j},\bar{r_k})}{n}\times 100\%$$

Where $r_{i,j}$ is the j-th response sample from the device d_i, $\bar{r_k}$ is the mean value of the N responses from the device d_k, n is the size of the response vector and HD represents the hamming distance. In other words, it corresponds to the average hamming distance between the reference signature of devices to the responses generated using the other devices to the same challenge. The optimal value for this indicator is **50%**.

2) Steadiness: For one device d_i, responses to one challenge c are expected to always be the same. Accordingly, steadiness represents the ability of a particular device to generate the same response to the same challenge and can be referenced as Intra-Chip variation (IC). This metric strongly depends on the environmental parameters, notably the temperature and the voltage.

$$IC_i(T,V) = \frac{1}{N}\sum_{j=1}^{N}\frac{HD(r_{i,j},r_{i,ref})}{n}\times 100\% \qquad (1)$$

Here, N represents the number of times the response is extracted from the device d_i. $r_{i,ref}$ is the mean value of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2017.2702607, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

responses of the same device d_i at the nominal temperature (T_n) and voltage (V_n). The optimal value of this indicator is **0%**.

3) Randomness: In contrast with the two first metrics, there is no specific formula to evaluate the randomness of PUFs. Traditionally, it is done by simply measuring the bias of the PUF responses, but this is obviously not sufficient. Indeed, if all responses contain as many zeros and one, a bias measure presents a perfect result even if there is a serious problem in the randomness of the PUF responses. For example, if the PUF responses is : 0101010101010101..., there is no bias but it is not random at all. Thus, there is an absolute need to find another way to evaluate the randomness of PUF responses.

To this end, we propose using a subset of the tests provided by the NIST statistical test suite (NIST SP 800-22 [30]). This subset is composed of six tests that can be performed using data of reduced length. However, the tests are designed to evaluate random number generators and not PUF so our confidence in the test results is limited. Indeed, when all six tests are passed successfully, this does not mean that the PUF responses are random, but if one of the tests fails, this demonstrates a serious lack of randomness and the configuration used to get the PUF response should be discarded. To better understand the six tests and how they can be used, each one is described below:

T1. The first test is called *mono-bit frequency test*. It measures the bias of a binary string.
T2. The second test performs the same operation but using different word sizes to compute the bias. The size of the word is a parameter m that can be set before starting the test,
T3. The third test measures the distance from 0 of a binary string. To do so, a number is fixed to 0 at the beginning of the test and the path of the binary string leads to addition (or subtraction) for each 1 (or 0). If the cumulative sums exceeds a threshold (fixed by the test), the test fails. The name of this test is *cumulative sums*,
T4. The fourth test evaluates the length of identical bit sequences inside the string. It corresponds to the *run test.*
T5. The fifth test aims to take a look at the irregularity of the longest string of 1 inside blocks (of length M) of the binary string. It corresponds to the *longest run of ones in a block test*,
T6. The sixth and last test is the *approximate entropy* test.

Thanks to those six statistical tests, it is possible to improve our understanding of the randomness of the PUF responses.

B. Parameters of the characterization

In addition to the three metrics presented in the previous section, a PUF needs to be evaluated under different operating conditions in order to prove its robustness. First, it is necessary to test the robustness of the environmental condition. This is even more true in the context of IoT where the devices can be placed in a wide variety of environments. In addition to the environmental parameters, we also include the acquisition window as a parameter. This new parameter has a huge impact on the quality of the PUF responses as demonstrated in Section IV-B3. Finally, we chose to use the Gray code to represent the PUF responses in order to limit the differences between consecutive values, as explained in the Section IV-B2.

1) Temperature and voltage: The first two parameters involved in a strong characterization of PUF are variations in the environmental temperature and variations in the power supply voltage. These types of variations are even more important in the context of IoT, where it is not possible to control the operating environment of billions of interconnected chips. To evaluate the steadiness of 128-bit chip IDs under different temperatures, all FPGAs are placed in a thermal oven (as shown in Figure 7) and the steadiness of the IDs built using the TERO-PUF responses is evaluated under different temperatures ranging from $-15°$ to $65°C$ increased in $10°C$ increments. Only results with temperature variations are presented for Xilinx Spartan 6 FPGAs in Section V. During characterization under temperature variations, all FPGAs are operating at their nominal voltage, which means 1.20 V for Xilinx Spartan 6 FPGAs.

Concerning variations in voltage, eight measurement points are selected around the nominal voltage of each FPGA and encompass the specifications of the FPGAs. In addition, two voltages among the eight are outside the voltage specifications. Thus, the six voltages in the Xilinx Spartan 6 specifications increase from 1.14 V to 1.26 V in 0.02 V increments and the two last voltages are 1.10 V and 1.30 V. For Altera Cyclone V FPGAs, the six voltages inside the specifications increase from 1.07 V to 1.13 V in 0.01 V increments and the two voltages outside the specifications are 1.05 V and 1.15 V. During the characterization of voltage variations, all FPGAs are placed in a controlled temperature environment at $25°$ C. To control the power supply of the FPGAs, a remotely programmable power supply is used.

2) The Gray code: As can be seen in Figure 5, the output of the subtracter is coded with the Gray code before the analysis of the PUF responses. We chose the Gray code because hamming distance (HD) between two consecutive numbers in Gray code is always equal to 1. This property makes this code very useful for the steadiness of the PUF responses. Conversely, the binary code can lead to errors in the analysis of steadiness. Indeed, if the mean of the difference between two TERO cells is around 2^n with $n \in \mathbb{N}$, a simple change of 1 in the value of the difference changes the PUF response completely because several bits of the response change. This is not the case using the Gray code because only one bit differs between two consecutive values. Let us illustrate this with $n = 5$, in the table II, bits which are modified between values 31 and 32 are in bold.

As can be seen in Table II, a change in one in the difference between the number of oscillations of two TERO cells can imply a significant HD in binary code that has a disastrous impact on the steadiness of the PUF responses. Conversely, the Gray code ensures a HD of one. Thus, the Gray code

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2017.2702607, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

Table II
EXAMPLE OF THE DIFFERENCE BETWEEN GRAY AND BINARY CODE FOR TWO CONSECUTIVE VALUES

Decimal value	Binary code	Gray code
$31 = 2^5 - 1$	00011111	00100000
$32 = 2^5$	00**100000**	0**1**100000
HD(31, 32)	6	1

makes it possible to really analyze the steadiness of the PUF responses. The steadiness becomes independent of how close the mean number of oscillations is to a 2^n value. Finally, the Gray code corresponds to a different representation of numbers and cannot be considered as an artificial improvement of the statistical properties of the PUF responses.

In addition, the Gray code divides a numeric value into three parts: the sign, the value, and some useless bits fixed at $'0'$ between the value and the sign. This property is interesting because it avoids choosing bits with the same information as the sign bit.

3) The acquisition window: This is a new parameter, never used in the state of the art of PUF characterization work to date. The choice to use it as a characterization parameter is based on the huge impact it has on the number of oscillations of the TERO cells. The acquisition window corresponds to the time during which we count the oscillations of the two selected TERO cells. This parameters can easily be changed by setting the time during which the *Init* signal (see Figure 5) is equal to 1.

After a first experiment using Xilinx Spartan 6 FPGAs with a very long acquisition window, we noticed that some TERO cells appeared to oscillate indefinitely. As a consequence, the response time of the TERO-PUF was very long. In the ideal case, these cells have to be discarded from the response generation scheme. However, changes in the steadiness and uniqueness of the PUF responses with respect to the acquisition window (Figure 6) showed that the uniqueness very quickly reached 50%, even though the TERO cells had not reached their stable state before the end of the acquisition window. Furthermore, Figure 6 shows that the shorter the acquisition window, the better the steadiness of the PUF responses.

Nevertheless, for the acquisition window, it is necessary to distinguish between three different cases:

- The first case is an acquisition window that is so short that no TERO cell can reach its stable state before the end of the acquisition window. In this case, the steadiness of the PUF responses is expected to be very good, but uniqueness will not be sufficient. Furthermore, a too short acquisition window implies that the behavior of the TERO-PUF will be identical to the behavior of the RO-PUF: only the frequencies of the cells can be used.
- The second case is an acquisition window that is long enough to let the majority of the TERO cells reach their stable state before it ends. This case is very interesting because it is not possible to know which cells will reach their stable state and which cells will still oscillating at the end of the acquisition window.
- The third and last case corresponds to a very long acquisition window and all TERO cells reach their stable state before it ends. If the mean number of oscillations of all the TERO cells is not too big, it corresponds to the ideal case, but if the mean number of oscillation is too big, the steadiness of the TERO cells will be not good enough and only the sign of the difference between the two selected cells could be used.

To illustrate this impact on the result of the PUF responses properties and the three aforementioned cases, the top panel in figure 6 shows the steadiness of signatures built using only the bits 4, 5, 6, 9 and 15 of the subtracter output. The bottom panel in figure 6 shows their uniqueness. To choose the bits represented in Figure 6, the values of the difference between the number of oscillations of TERO cells were analyzed to select three bits used to represent the numeric values with a short acquisition window (bit 4, 5 and 6), the sign bit (bit 15) and one bit used to represent the value only using a long acquisition window (bit 9).

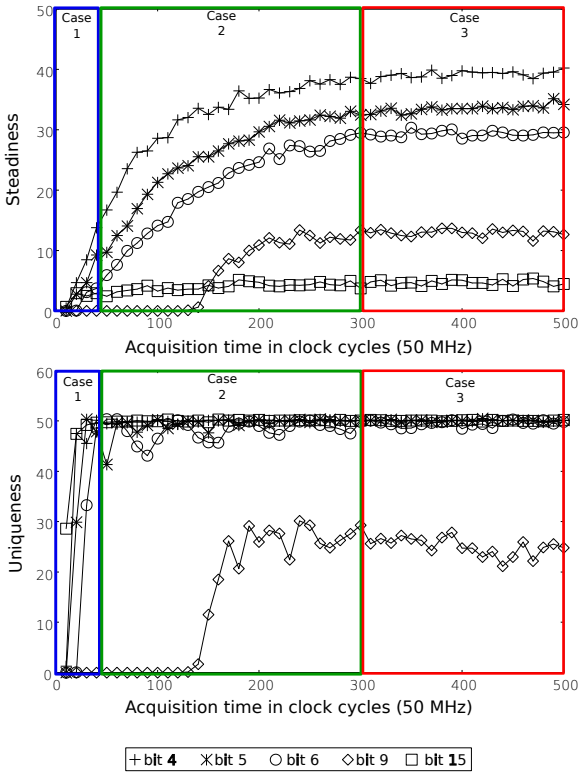

Figure 6. Changes in steadiness and uniqueness with variations in acquisition time.

V. COMPARISON OF CHARACTERIZATION RESULTS

A. Experimental setup

All the results presented in this section were generated from 30 Xilinx Spartan 6 FPGAs (XC6SLX16CSG324-3) and from 18 Altera Cyclone V FPGAs (EP5CEBA4F17C8N). Figure 7 shows the test bench built to characterize the PUFs. As can be seen, it uses a platform where it is possible to connect six boards at a time. This has the advantage of making the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2017.2702607, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

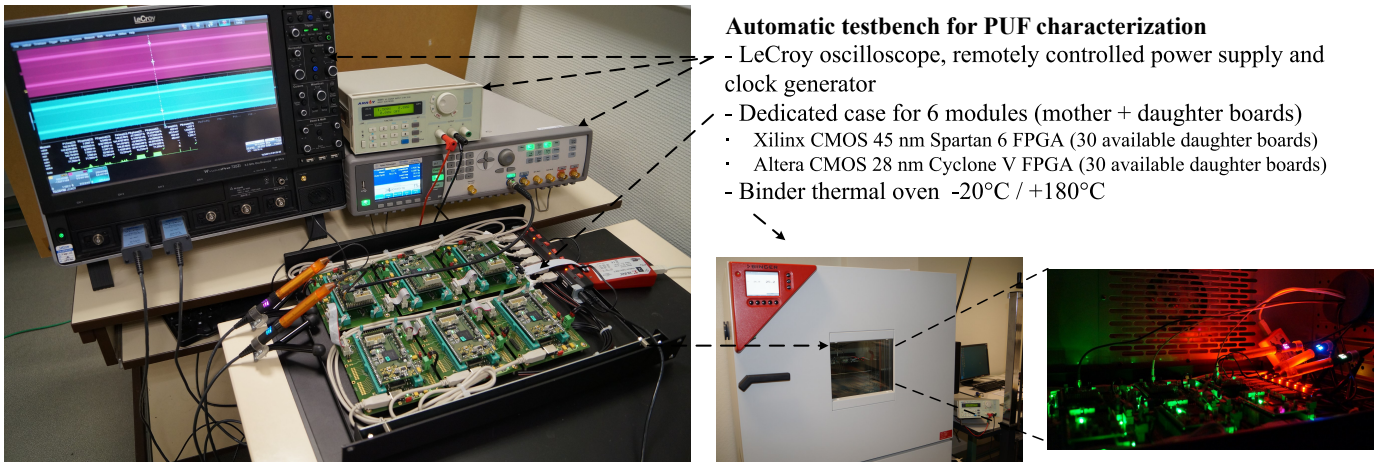

Figure 7. Test bench used to characterize the TERO-PUF

characterization faster since it can be done on several boards simultaneously. In addition, using the exact same experimental setup to characterize different PUFs in different technologies ensures the comparison is fair.

All PUF responses generated in this section are 128 bits long. The acquisition system uses two 16-bit counters to extract the number of oscillations of the TERO cells. The bit referenced as Bit 0 represents the least significant bit and the one referenced as Bit 15 represents the most significant bit of the subtracter output.

B. Choice of the bits to use with Xilinx Spartan 6 FPGAs

Now all the parameters are known, it is possible to choose which bits to use to build chip ID. To this end, a first experiment was performed on Xilinx Spartan 6 FPGAs working at a temperature of 25° C and nominal voltage. The acquisition time was set to 30 clock cycles at 50 MHz. In this experiment, chip IDs were built using only one bit of the subtracter output, and steadiness and uniqueness were analyzed. Table III presents the results of this first experiment. Each result corresponds to the means of steadinesses and uniqueness over 30 FPGAs.

Table III
UNIQUENESS AND STEADINESS OF CHIP ID OF 128 BITS BUILT USING ONE BIT OF THE SUBTRACTER OUTPUT ON XILINX SPARTAN 6 FPGAS WORKING AT NOMINAL TEMPERATURE AND VOLTAGE CONDITIONS AND USING AN ACQUISITION WINDOW OF 30 CLOCK CYCLES AT 50 MHZ

Bit	Uniqueness (%)	Steadiness (%)
0	47.65	28.41
1	42.37	23.02
2	41.92	15.86
3	42.33	10.09
4	40.04	5.04
5	45.56	2.16
6	27.03	1.40
7	0.04	0.04
8	0	0
...	...	...
15	48.46	2.63

By fixing an arbitrary threshold at 10%, it is possible to select the bit configurations that can be used as signatures. This threshold is fixed arbitrarily and can be changed depending on the target application. In the rest of this paper, we assume that 10% is a reasonable threshold since no error correction will be performed on chip. Indeed, to authenticate a device, there is no need for one hundred percent steadiness and the error correction should be included in the server or in the authentication protocol [31]. In this case, Table III shows that three bits can be used to build chip ID using the TERO-PUF on Xilinx Spartan 6 FPGA: bit 4, bit 5 and bit 15. This choice depends to a great extent on the technology and on the settings of the experiment, especially acquisition time. Finally, it is possible to see that after bit 5, the uniqueness of the built signature falls drastically, which means that these bits will not be used to represent the difference between the numbers of oscillations of the selected TERO cells.

The same experiment was done to select the bits that can be used with Altera Cyclone V FPGAs and for an acquisition time of 30 clock cycles at 50 MHz: the bits are bit 5, bit 6 and bit 15.

C. Robustness of Xilinx Spartan 6 characterization

To present the characterization results of the TERO-PUF implemented in the Xilinx Spartan 6, a classical approach was used: the steadiness of the responses for the different temperature and voltage are given for the most interesting bits. For the RO-PUF, only the sign bit (Bit 15) was used, but due to the transient effect of the TERO-PUF, it is possible to extract between two and three bits per challenge instead of one. Figure 8 gives the results of the robustness to variations in temperature and Figure 9 gives results of the robustness to variations in voltage. In both graphs, results are presented for bits 4, 5 and 15. The combination of bits 5 and 15 and of bits 4, 5 and 15 are also presented. These results were generated using an acquisition window of 30 clock cycles at 50 MHz.

According to Figure 8, the steadiness of the worst response is less than 10% between 15° C and 35° C, which corresponds to a variation of 40% around $T_n = 25°$ C for variations in temperature. Figure 9 shows that the steadiness of the responses is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2017.2702607, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

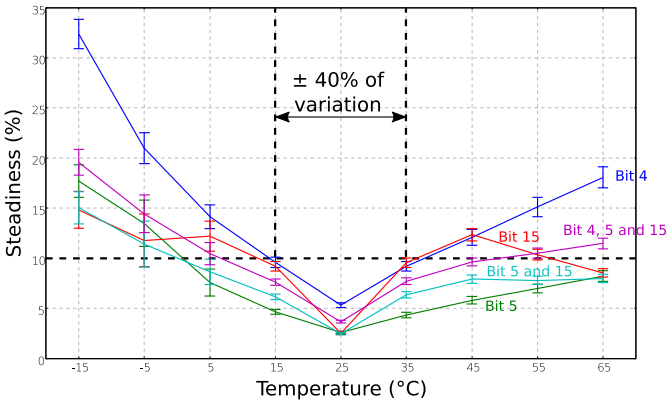

Figure 8. Evaluation of the robustness of the TERO-PUF responses to variations in temperature using an acquisition window of 30 clock cycles at 50 MHz on Xilinx Spartan 6 FPGAs

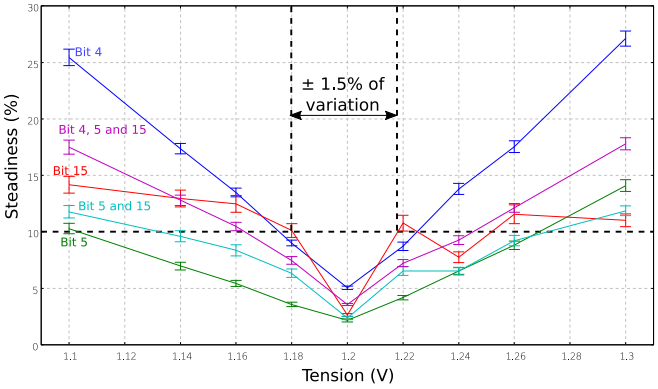

Figure 9. Evaluation of the robustness of the TERO-PUF responses to variations in voltage using an acquisition window of 30 clock cycles at 50 MHz on Xilinx Spartan 6 FPGAs.

less than 10% only between 1.18 V and 1.22 V for variations in voltage, which corresponds to a variation of 1.5 % around $V_n = 1.2$ V. Thus, the sensitivity of TERO-PUF to variations in temperature is low, but it is more sensitive to variations in voltage. The worst responses correspond to those generated using only bit 4 of the subtracter output for robustness to variations in temperature and to responses generated using bit 15 of the subtracter output for the robustness to variations in voltage. All the other configurations gave better results as can be seen in Figure 8 and Figure 9.

It is now important to take a look at the randomness of the generated responses. To this end, the six tests presented in Section IV-A3 were performed and the results are presented in Table IV. For the results of the block frequency test (T2), the size of the block taken to compute the frequency was set to the number of bits selected to generate the response. Thus, if only one bit is used to generate the PUF responses, this test is exactly the same as the frequency test (T1). In Table IV, an empty box means the test failed, and an X in a box means the test succeeded. If *na* is written in a box, the test was not applied. The steadiness and the uniqueness at the nominal operating condition (25° C and 1.2 V) are also shown in Table IV.

Table IV
EVALUATION OF THE RANDOMNESS THE THE TERO PUF RESPONSES GENERATED USING 1 TO 3 BITS PER CHALLENGE WITH AN ACQUISITION WINDOW OF 30 CLOCK CYCLES AT 50 MHZ ON XILINX SPARTAN 6 FPGAS

Bit selected	Steadiness %	Uniqueness %	Statistical tests					
			T1	T2	T3	T4	T5	T6
Bit 4	5.31	41.72		na				
Bit 5	2.60	46.49		na				
Bit 15	2.50	48.48		na			X	
Bits 5 & 15	2.46	47.83		X		X	X	X
Bits 4, 5 & 15	3.67	46.60		X		X	X	

As can be seen in Table IV, no configuration successfully passed all six tests. This means that the statistical properties of the TERO-PUF responses generated using an acquisition window of 30 clock cycles at 50 MHz are not good enough to be used. The best configuration corresponds to the one using bits 5 and 15 to generate the responses, which means that it is possible to extract more than one bit per challenge with the TERO-PUF. However, the results of the statistical test indicate that the acquisition window of 30 clock cycles at 50 MHz is probably too short to be used with Xilinx Spartan 6 FPGA. This acquisition window will be part of case one presented in Section IV-B3.

To check that it is truly possible to extract more than one bit per challenge and to generate responses with satisfactory steadiness, uniqueness and randomness, a second characterization was performed at nominal condition using an acquisition window of 60 clock cycles at 50 MHz. This time, the interesting bits were bit 5, 6 and the sign bit (bit 15). The results of the six statistical tests, the steadiness and the uniqueness of the second characterization are presented in Table V.

Table V
EVALUATION OF THE RANDOMNESS THE THE TERO PUF RESPONSES GENERATED USING 1 TO 3 BITS PER CHALLENGE WITH AN ACQUISITION WINDOW OF 60 CLOCK CYCLES AT 50 MHZ ON XILINX SPARTAN 6 FPGAS

Bit selected	Steadiness %	Uniqueness %	Statistical tests					
			T1	T2	T3	T4	T5	T6
Bit 5	10.17	49.88	X	na	X	X	X	X
Bit 6	5.09	49.88	X	na	X	X	X	X
Bit 15	2.38	49.37	X	na	X	X	X	X
Bits 5 & 15	6.08	49.51	X	X	X	X	X	X
Bits 6 & 15	3.68	49.65	X	X	X	X	X	X
Bits 5, 6 & 15	5.89	49.49	X	X	X	X	X	X

In contrast to the results obtained using an acquisition window of 30 clock cycles at 50 MHz, Table V shows that all responses generated using an acquisition window of 60 clock cycles at 50 MHz successfully passed the six statistical tests. Moreover, only responses generated using the bit 5 of the difference between the number of oscillations of the TERO cells presents a steadiness higher than 10%. Thus, it is possible to generate responses using one, two or three bits of the difference between the number of oscillations of the TERO cells using this acquisition window. In particular, the configuration using bit 6 and bit 15 shows very good steadiness (3.68%) and uniqueness (49.65%).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2017.2702607, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

D. Robustness of the Altera Cyclone V characterization

Only variations in voltage were available for the characterization of the TERO-PUF on Altera Cyclone V FPGAs because we had an unexpected problem with the power supply of the FPGAs which led to errors during the characterization of variations in temperature. The problem is now solved but due to the deadline for the submission of this paper, the characterization of the TERO-PUF with respect to variations in temperature on Altera Cyclone V FPGAs will be conducted in a future work. Meanwhile, this section presents the results of the characterization of the TERO-PUF with respect to variations in voltage on Altera Cyclone V FPGAs. Exactly like the characterization on Xilinx Spartan 6 FPGAs, it is possible to extract from one to three bits per challenge. Figure 10 shows the results of the characterization of variations in voltage using an acquisition window of 30 clock cycles at 50 MHz. In Figure 10, characterization results are presented for responses generated using bit 5, 6 and 15. The combination of bits 5 and 15, bits 6 and 15 and the combination of bits 5, 6 and 15 are also presented.

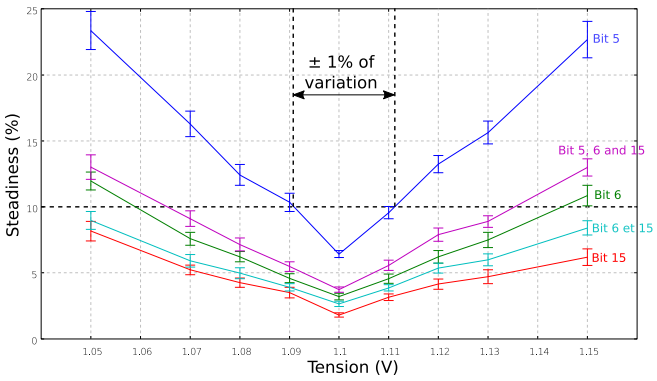

Figure 10. Evaluation of the robustness of the TERO-PUF responses to variations in voltage using an acquisition window of 30 clock cycles at 50 MHz on Altera Cyclone V FPGAs

As can be seen in Figure 10, the less stable responses correspond to those generated using bit 5 of the difference in the number of oscillations. Indeed, these responses were less than 10% only between 1.09 V and 1.11 V, which represents a variation of 1% around the nominal voltage (1.10 V). Nevertheless, all the other configurations used to generate responses showed a steadiness of less than 10% for all the voltage specifications (from 1.07 V to 1.13 V). This thus confirms that it is possible to extract more than one bit per challenge with the TERO-PUF on Altera Cyclone V FPGAs.

The last step of the characterization is to take a look at the randomness of the generated responses. To this end, responses were generated under nominal operating conditions (1.1 V and 25° C) and the six tests presented in Section IV-A3 were performed. Table VI shows the results of these statistical tests for an acquisition window of 30 clock cycle at 50 MHz.

Table VI
EVALUATION OF THE RANDOMNESS OF THE TERO PUF RESPONSES GENERATED USING 1 TO 3 BITS PER CHALLENGE WITH AN ACQUISITION WINDOW OF 30 CLOCK CYCLES AT 50 MHZ ON ALTERA CYCLONE V FPGAS

Bit selected	Steadiness %	Uniqueness %	Statistical tests					
			T1	T2	T3	T4	T5	T6
Bit 5	6.42	45.88		na				
Bit 6	3.21	50.09	X	na	X	X	X	X
Bit 15	1.80	47.62	X	na	X	X	X	X
Bits 6 & 15	2.66	48.58	X	X	X	X	X	X
Bits 5, 6 & 15	3.73	47.39	X	X	X	X	X	X

As can be seen in Table VI, only two response configurations did not pass the six tests: bit 5 and bits 5 and 15. All the others successfully passed the six statistical tests. Furthermore, the responses generated using bits 6 and 15 and the responses generated using bits 5, 6 and 15 had good statistical properties as well as good steadiness and uniqueness. This confirms that the TERO-PUF makes it possible to extract several bits per challenge. Last but not least, the acquisition window of 30 clock cycles at 50 MHz does not seem to be too narrow with Altera Cyclone V FPGAs as was the case for Xilinx Spartan 6 FPGAs.

E. Summary and comparison of the results

The results of the characterization for Altera Cyclone V FPGAs are very similar to the results obtained for Xilinx Spartan 6 FPGAs. Nevertheless, it is interesting to analyze results from a different and more industrial perspective. Let us assume that the expected robustness to variations in temperature and in voltage represents a budget and let us assume that this budget is 10%. Now, to characterize the TERO-PUF, ranges of temperature and voltage are required that ensure that the steadiness of the TERO-PUF is below the 10% budget. This approach is even more interesting because it makes it possible to know the maximum number of errors for which the PUF responses will have to choose the appropriate error correcting scheme, if required.

Table VII summarizes all the results of the characterization of the two FPGAs technologies using this constraint approach. In addition, uniqueness is given in this table. It is possible to see the consistency of the TERO-PUF results with different technologies. Furthermore, the ranges of robustness to variations in voltage encompass the full specifications of each technology used in this article. Accordingly, the best configuration to generate signatures using the TERO-PUF in these two FPGA technologies extracts 2 bits per challenge (in bold in Table VII).

To extend this comparison, we implemented and characterized a RO-PUF on Xilinx Spartan 6 and Altera Cyclone V FPGAs. The results of this characterization are given in Table VIII. The results of other studies on RO-PUF and TERO-PUFs are included [32], [33], [24] and [27]. For each PUF, the size of the basic cell (RO or TERO) is explicitly indicated in Table VIII. The table shows the uniqueness and steadiness at nominal condition as well as the worst case steadiness, which is the least stable point of the PUF with respect to variations in voltage and temperature. Concerning the variations in temperature used to characterize the RO-PUF implemented,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2017.2702607, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

Table VII
COMPARISON OF THE RESULTS OF THE CHARACTERIZATION OF THE TERO-PUF ON XILINX SPARTAN 6 AND ALTERA CYCLONE V FPGAS

Response bit per challenge	Steadiness mean		Uniqueness		Range constraint	T°range		Voltage range	
	Spartan 6	Cyclone V	Spartan 6	Cyclone V		Spartan 6	Cyclone V	Spartan 6	Cyclone V
1	2.63%	1.80%	48.46%	47.62%	10%	2°C to 65°C	na	1.10 V to 1.27 V	1,05 V to 1,15 V
2	**2.46%**	**2.66%**	**47.83%**	**48.58%**	10%	**2°C to 65°C**	na	**1.14 V to 1.27 V**	**1,05 V to 1,15 V**
3	3.67%	3.73%	46.60%	47.39%	10%	5°C to 48°C	na	1.16 V to 1.25 V	1,06 V to 1,13 V

we chose a wider range of variations, from $-15°$ C to $65°$ C. For variations in voltage, the measurements were from 1.05 V to 1.15 V for Altera Cyclone V FPGAs and from 1.1 V to 1.30 V for Xilinx Spartan 6 FPGAs.

As can be seen in Table VIII, the RO-PUF appears to be more robust to ASIC than on FPGA as also demonstrated by the work presented in [33] regarding the result of [32] and our results on RO-PUF. The RO-PUF shows very good steadiness on Altera Cyclone V FPGA compared to the TERO-PUF. Concerning the steadiness on Xilinx Spartan 6 FPGAs, the two PUF present very similar results. For the two types of PUF, note that increasing the number of inverters in the basic cell improves robustness to environmental variation. However, this also slightly increases steadiness in normal operating conditions. Thus, the size of the basic cells for a given technology is a trade off between the steadiness and the robustness of the PUF.

Finally, the TERO-PUF makes it possible to extract from 1 to 3 bits per challenge. In addition, the uniqueness of TERO-PUF is better than that of RO-PUF, which means that the TERO-PUF extracts more entropy from variations in the manufacturing process than the RO-PUF.

VI. THE TERO-PUF FOR IOT

Let us consider a small IoT environment such as a smart home where numerous devices are linked together. This kind of environment makes it possible to remotely control the heater, lights and many other devices using a single smartphone. With no limits on control and access, anyone could control our devices. Now assuming that each device of the IoT is composed of an unique ID and only the ones stored during an initialization phase are able to communicate and control other devices, the system is much more secure.

That is why it is indispensable to be able to authenticate, control access and provide traceability in this kind of application. As mentioned above, all these features are possible using a PUF. The efficiency of RO-PUF has been proven several times and it turns out to be one of the best candidates for implementation in both FPGA and ASIC. Indeed, it is a suitable PUF for both in terms of feasibility, cost and efficiency. However, the RO-PUF has security problems since it can be cloned [22] and is subject to locking phenomena [24].

In section V, we show that the TERO-PUF achieves similar results to RO-PUF in terms of statistical quality. In addition, thanks to temporary oscillation, the TERO-PUF is more robust to electromagnetic attacks, insensitive to the locking phenomenon and consumes less power than the RO-PUF. Indeed, the locking phenomena correspond to the manipulation of the frequency of oscillating cell in order to force them to operate at a particular frequency. More explanation of this can be found in [22]. Since the principle of the RO-PUF is based on the frequency mismatch of theoretically identical cells, lock them to the same frequency becomes a real issue. In the case of the TERO-PUF, it is not the frequency but the number of transient oscillations that is analyzed. In addition, the number of oscillations is finite and the oscillating time is usually short. This implies that the locking phenomena will not have an impact on the TERO-PUF. Last but not least, the TERO-PUF makes it possible to extract several bits per challenge, which leads to area efficiency. The TERO-PUF is consequently lighter than the RO-PUF in terms of area and power consumption [34]. All these reasons make the TERO-PUF a better primitive for IoT than the RO-PUF.

Finally, PUFs need to be used to authenticate devices. Thus, there is no need for 100% steadiness. Indeed, using lightweight protocols ([35], [31]), a device can be authenticated without perfect steadiness. In addition, if an error correction is needed to authenticate devices, it has to be implemented in the authenticating server and not on chip, especially in the context of IoT where area and power are two important constraints.

VII. CONCLUSION

In this paper, TERO-PUF implementations are described for two different FPGA families, Xilinx Spartan 6 and Altera Cyclone V. These implementations represent designs made at the lowest possible level accessible for both families. In addition, the results of characterization are given for both implementations. Characterization was performed using the exact same set up and the exact same global system. The comparable results prove that the TERO-PUF is reliable and not very sensitive to variations in temperature and voltage. As a result, this PUF can be used as the only identifier in the context of IoT, which includes heterogeneous devices originating from different technologies and operating under many different environmental conditions.

The TERO-PUF makes it possible to extract several bits per challenge with no loss of statistical characteristics. A further advantage that makes this PUF a serious candidate for IoT usages is that it is both rapid and lightweight.

ACKNOWLEDGMENTS

This work was conducted in the framework of the SALWARE project number ANR-13-JS03-0003 supported by the French "*Agence Nationale de la Recherche*" and by the French "*Fondation de Recherche pour l'Aéronautique et l'Espace*". This work also received funding from the European Union

Table VIII
COMPARISON OF THE TERO-PUF WITH OTHER TECHNOLOGIES AND PUFS

Metric	RO-PUF [32]	RO-PUF [33]	TERO-PUF [24]	TERO-PUF [27]	TERO-PUF		RO-PUF	
Technology	Xilinx Spartan-3E ($90nm$)	ASIC ($65nm$)	Altera Cyclone-II ($90nm$)	ASIC ($350nm$)	Xilinx Spartan-6 ($45nm$)	Altera Cyclone-V ($28nm$)	Xilinx Spartan-6 ($45nm$)	Altera Cyclone-V ($28nm$)
Uniqueness	47.3%	49.5%	48.0%	49.7%	48.5%	47.6%	55.5%	55.3%
Nominal steadiness	0.9%	2.8%	1.7%	0.6%	2.6%	1.8%	2.5%	0.5%
Worst case steadiness (regarding temperature and voltage variations)	15%	3.9%	na	6.2%	15%	8%	5.5%	6.5%
Architecture of the basic cell	1 NAND and 4 inverters	1 NAND and 40 inverters	2 NAND and 14 inverters	2 NAND and 14 inverters	2 AND and 14 inverters	2 AND, 2 inverters and 12 LCELL	1 AND and 3 inverters	1 AND and 3 inverters

Horizon 2020 research and innovation programme in the framework of the project HECTOR (Hardware Enabled Cryptoand Randomness) under grant agreement $N°644052$. The authors wish to thanks Pauline Bondon for her valuable help in designing the TERO cell in Altera FPGA. Serigne Sarr is also gratefully acknowledged for characterization of the RO PUF on Altera Cyclone V and Xilinx Spartan 6 FPGAs.

REFERENCES

[1] "http://energy.gov/sites/prod/files/2015/04/f22/bosch

[2] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of iot systems: Design challenges and opportunities," in *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design*, ser. ICCAD '14. Piscataway, NJ, USA: IEEE Press, 2014, pp. 417–423. [Online]. Available: http://dl.acm.org/citation.cfm?id=2691365.2691450

[3] D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497 – 1516, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870512000674

[4] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146 – 164, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128614003971

[5] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2010.05.010

[6] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, "Vision and challenges for realising the internet of things," *Cluster of European Research Projects on the Internet of Things, European Commision*, 2010.

[7] R. Anderson and M. Kuhn, *Low cost attacks on tamper resistant devices*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 125–136. [Online]. Available: http://dx.doi.org/10.1007/BFb0028165

[8] K. Kursawe, D. Schellekens, and B. Preneel, "Analyzing trusted platform communication," in *ECRYPT Workshop, CRASH-CRyptographic Advances in Secure Hardware*. Citeseer, 2005.

[9] A. Cherkaoui, L. Bossuet, L. Seitz, G. Selander, and R. Borgaonkar, "New paradigms for access control in constrained environments," in *9th International Symposium on Reconfigurable and Communication Centric Systems-on-Chip (ReCoSoC)*, 2014.

[10] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions," *IACR Cryptology ePrint Archive*, 2011.

[11] 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*, 2009.

[12] F. Tehranipoor, N. Karimian, W. Yan, and J. A. Chandy, "Dram-based intrinsic physically unclonable functions for system-level security and authentication," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. PP, no. 99, pp. 1–13, 2016.

[13] S. Sutar, A. Raha, and V. Raghunathan, "D-puf: An intrinsically reconfigurable dram puf for device authentication in embedded systems," in *Proceedings of the International Conference on Compilers, Architectures and Synthesis for Embedded Systems*, ser. CASES '16. New York, NY, USA: ACM, 2016, pp. 12:1–12:10. [Online]. Available: http://doi.acm.org/10.1145/2968455.2968519

[14] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Lightweight secure pufs," in *In Proc. of the IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2008.

[15] A. Maiti and P. Schaumont, "Improved ring oscillator puf: An fpga-friendly secure primitive," *Journal of Cryptology*, 2011.

[16] Z. Cherif, J.-L. Danger, S. Guilley, and L. Bossuet, "An easy-to-design puf based on a single oscillator: The loop puf," in *Euromicro Conference on Digital System Design (DSD)*, 2012.

[17] B. Habib, J. Kaps, and K. Gaj, "Efficient sr-latch PUF," in *Applied Reconfigurable Computing - 11th International Symposium, ARC 2015, Bochum, Germany, April 13-17, 2015, Proceedings*, 2015, pp. 205–216. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-16214-0_17

[18] S. Morozov, A. Maiti, and P. Schaumont, "An analysis of delay based PUF implementations on FPGA," in *In Proc. of the 6th International Symposium on Reconfigurable Computing: Architectures, Tools and Applications (ARC)*, 2010.

[19] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A large scale characterization of RO-PUF," in *In Proc. of the 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2010.

[20] A. Maiti, V. Gunreddy, and P. Schaumont, "A framework for the evaluation of physical unclonable functions," *in Proc. of NIST Work. on Crypto. For Emerging Tech. and Appl.*, 2011.

[21] L. Feiten, A. Spilla, M. Sauer, T. Schubert, and B. Becker, "Analysis of ring oscillator pufs on 60nm fpgas," *European cooperation in science and technology*, 2013.

[22] P. Bayon, L. Bossuet, A. Aubert, and V. Fischer, "Electromagnetic analysis on ring oscillator-based true random number generators," in *2013 IEEE International Symposium on Circuits and Systems (ISCAS2013), Beijing, China, May 19-23, 2013*, 2013, pp. 1954–1957.

[23] P. Maistri, R. Leveugle, L. Bossuet, A. Aubert, V. Fischer, B. Robisson, N. Moro, P. Maurine, J. M. Dutertre, and M. Lisart, "Electromagnetic analysis and fault injection onto secure circuits," in *2014 22nd International Conference on Very Large Scale Integration (VLSI-SoC)*, Oct 2014, pp. 1–6.

[24] L. Bossuet, X. T. Ngo, Z. Cherif, and V. Fischer, "A puf based on a transient effect ring oscillator and insensitive to locking phenomenon," *IEEE Transactions on Emerging Topics in Computing*, 2014.

[25] L. M. Reyneri, D. D. Corso, and B. Sacco, "Oscillatory metastability in homogeneous and inhomogeneous flip-flops," *IEEE Journal of Solid-State Circuits*, 1990.

[26] M. Varchola, M. Drutarovský, and V. Fischer, "New universal element with integrated puf and trng capability," in *International Conference on Reconfigurable Computing and FPGAs (ReConFig)*, 2013.

[27] A. Cherkaoui, L. Bossuet, and C. Marchand, "Design, evaluation, and optimization of physical unclonable functions based on transient effect ring oscillators," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1291–1305, June 2016.

[28] http://www.xilinx.com/support/documentation/sw_manuals/xilinx14_7/spartan6_hdl.pdf.

[29] "http://www.univ-st-etienne.fr/salware/tero_puf.htm."

[30] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," DTIC Document, Tech. Rep., 2001.

[31] B. Colombier, L. Bossuet, D. Hély, and V. Fischer, "Key reconciliation protocols for error correction of silicon puf responses," 2016.

[32] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A large scale characterization of RO-PUF," in *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on*, June 2010, pp. 94–99.

[33] R. Maes, D. Schellekens, and I. Verbauwhede, "A Pay-per-Use Licensing Scheme for Hardware IP Cores in Recent SRAM-Based FPGAs," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 1, pp. 98–108, 2012.

[34] U. Mureddu, L. Bossuet, and V. Fischer, "A comparison of PUF cores suitable for FPGA devices," Conference on trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE), Nov. 2016, poster. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01382987

[35] J. Delvaux, D. Gu, D. Schellekens, and I. Verbauwhede, "Secure lightweight entity authentication with strong pufs: Mission impossible?" *Cryptographic Hardware and Embedded Systems (CHES)*, 2014.

Cédric Marchand received a master degree (2013) in microelectronics and embedded systems from the École Nationale Supérieur des Mines de Saint-Etienne (ISMIN), Gardanne, France. He received the Ph.D degree (2016) in microelectronic from the University of Lyon, Saint-Etienne, France. His thesis received the prize of excellence of the University Jean-Monnet foundation in 2017. Since the end of 2016, he is Post doctoral researcher in the Secure Embedded System Group at the Hubert Curien Laboratory. His main research activities focus on embedded systems hardware security, side channel attacks of cryptographic circuits, Internet of things security and reconfigurable architecture for security.

Lilian Bossuet was a student of the prestigious Ecole Normale Supérieure de Cachan, France. He received the M.S. degree (2001) in electrical engineering from the Institut National des Sciences Appliquées, Rennes, France, and the Ph.D. degree (2004) in electrical engineering and computer sciences from the University of South Britanny, Lorient, France. From 2005 to 2010, he has been an Associate Professor, and the head of the Embedded System Department in the Bordeaux Institute of Technologies. Since 2010, he is Associate Professor at the University of Lyon/Saint-Etienne and he is a member of the Hubert Curien Laboratory. He holds the special CNRS (Centre National de la Recherche Scientifique) Chair of Applied Cryptography and Embedded System Security. He is the head of the Secure Embedded System group and the head of the computer sciences Department of the Hubert Curien Laboratory. His main research activities focus on embedded systems hardware security, IP security, IC security, side channel attacks of cryptographic circuits, CryptoProcessor design, and reconfigurable architecture for security. Lilian is a member of the IEEE and a senior member of the CryptArchi Club.

Ugo Mureddu received the M.Sc. degree (2015) in electronics and embedded systems from "Institut National des Sciences Appliquées", Lyon, France and the M.Sc. degree (2015) in embedded systems and telecommunication engineering from "Telecom Saint-Etienne", Saint-Etienne, France. He is currently a second year Ph.D. student in Hubert Curien Laboratory, University of Lyon. His research interests include hardware security.

Nathalie Bochard is a research engineer at the CNRS (Centre National de Recherche Scientifique). She received the masterâĂŹs degree in electronic engineering in 1996 and the diploma of technological research (DRT) in vision, telecommunications and instrumentation from the University of Lyon, in 1997. She joined the CNRS (the official French research institution) in 1998, first at its laboratory Service Central dâĂŹAnalyses in Lyon, and since 2001 at the Hubert Curien Laboratory in St-Etienne. Currently, her main research interests include embedded hardware cryptographic architectures for configurable logic devices and especially design, implementation and evaluation of true random number generators and physical unclonable functions aimed at cryptographic applications.

Abdelkarim Cherkaoui is a post-doctoral researcher at TIMA laboratory and Grenoble INP. He received his M.S. degree in Microelectronics from Joseph Fourier University in Grenoble (2010), and he completed his PhD in applied cryptography in Hubert Curien laboratory at Saint-Etienne (2014). His research activities cover two main topics: hardware security and asynchronous design techniques for ultra-low power devices.

Viktor Fischer received the M.S. and Ph.D. degrees in electrical engineering from the Technical University of Kosice, Slovakia. From 1981 to 1991, he held an Assistant Professor position at the Department of Electronics, Technical University of Kosice. From 1991 to 2006, he was a part-time Invited Professor at the University of Saint-Etienne, France. From 1999 to 2006, he was a consultant with Micronic Slovakia, oriented in hardware data security systems. Since 2006, he has been a full-time Professor at the University of Saint-Etienne. His research interests include cryptographic engineering, secure embedded systems, cryptographic processors and especially true random number generators embedded in logic devices. He is the co-founder and senior member of the CryptArchi club.