HAL open science

Identification of Hardware Devices based on Sensors and Switching Activity: a Preliminary Study

Honorio Martin, Elena Ioana Vatajelu, Giorgio Di Natale

To cite this version:

Honorio Martin, Elena Ioana Vatajelu, Giorgio Di Natale. Identification of Hardware Devices based on Sensors and Switching Activity: a Preliminary Study. Design, Automation & Test in Europe Conference & Exhibition (DATE 2021), Feb 2021, Grenoble (virtuel), France. 10.23919/DATE51398.2021.9474173 . hal-03351477

HAL Id: hal-03351477

https://hal.science/hal-03351477v1

Submitted on 22 Sep 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution - NonCommercial 4.0 International License

Identification of Hardware Devices based on Sensors and Switching Activity: a Preliminary Study

Honorio Martin[1], Elena-Ioana Vatajelu[2], Giorgio Di Natale[2]

[1]University Carlos III of Madrid, Madrid, Spain
[2]Univ. Grenoble Alpes, CNRS, Grenoble INP*, TIMA, 38000 Grenoble, France

***Abstract*—Hardware device identification has become an important feature for enhancing the security and the trust of interconnected objects. In this paper, we present a device identification method based on measuring physical and electrical properties of the device, while controlling its switching activity. The method is general an applicable to a large range of devices from FPGAs to processors, as long as they embed sensors (such as temperature and voltage) and their measurements are available. The method is enabled by the fact that both the sensors and the effects of the switching activity on the circuit are uniquely affected by manufacturing-induced process variability. The device identification based on this method is made possible by the use of machine learning. The efficiency of the method has been evaluated by a preliminary study conducted on eleven FPGAs.**

***Index Terms*—device fingerprinting, on-chip sensors,switching activity, ring-oscillator, FPGA, neural network.**

I. Introduction

Device fingerprinting, consisting on obtaining a set of attributes from a device, can be a powerful mechanism for device identification [1]. This identification technique is widely used for Web tracking and fraud prevention and there are many different hardware and software techniques described in the literature. For device identification, the fingerprint should be as immutable as possible and thus hardware-based solutions are preferred. In this context, the use of sensors has emerged as an attractive solution for different platforms. The greatest exponent of this trend is the use of mobile phone sensors such as accelerometers, gyroscopes or microphones [2]. These systems need to generate a known stimulus and the response of the sensors to that stimulus will identify the device. Nevertheless, to the best of our knowledge, solutions based on sensors embedded in microprocessors, FPGAs or GPUs (typically temperature and voltage sensors) have not been explored.

In this paper, we propose a device identification method based on measuring physical and electrical properties of the device, while controlling its switching activity. The method is enabled by the fact that both the sensors and the effects of the switching activity on the circuit are uniquely affected by manufacturing-induced process variability.

The rest of the paper is organised as follows. In Section II, the proposed hardware device identification method is described, while the experimental set-up used to demonstrate the feasibility of the proposed method is presented in Section III. In Section IV are presented the experimental results, including the results related to the identification accuracy on different scenarios. Finally, some conclusions and recommendations are drawn in Section V.

This work has been partially funded by the CNRS INS2I PUF2IOT 2020 projet and the UC3M program: Ayudas para la Movilidad del Programa Propio de Investigación

*Institute of Engineering Univ. Grenoble Alpes

II. Proposed identification scheme

On-chip sensors are embedded elements widely deployed in many computing systems (e.g. MCUs, GPUs, FPGAs,etc.) which allow self-regulation of operation conditions. Among the most commonly used sensors are the temperature sensors and the voltage sensors (core voltage, power supply noise, etc.). The measurements recorded by these sensors are strongly dependent on the electric activity of the hosting device. As a rule of thumb, increased activity in the vicinity of the sensors can be observed as a temperature increase, as disturbance in the core voltage, etc. The exact values of these measurements are influenced by the fabrication-induced process variability affecting the sensors, which can induce effects like simple linear bias (like offset) or more complex effects such as cross-dimensional effects, clock-skew, tolerance or timing bias [3]. Moreover, the electric activity of the hosting device depends on the switching activity and it is highly affected by the fabrication-induced parametric variations of the underling circuit. Therefore, the measurements from the embedded sensors are doubly affected by the fabrication-induced process variability.

The proposed identification method is based on this double effect (variability on the circuit, plus variability on the sensors measuring properties of the circuit), which results in unique features that can be used to construct a reliable hardware fingerprint of devices. In a nutshell, we generate a specific workload using different elements of the system and we record the measurements of the on-chip sensors of the system. This, in turn, allows us to build a completely self-contained fingerprinting scheme. Nevertheless, modeling the impact of the switching activity on the on-chip sensor measurements is a very challenging task. Such a model depends on many factors, as the initial state of the system, the workload, the physical location of the switching elements and on-chip sensors, crosstalk effects and the imperfections of the device. Because of the aforementioned model complexity, we propose the use of an artificial neural network (ANN) for device classification. The input of the ANN will be the raw on-chip sensor measurements generated during the application of a specific workload, while the output is the device ID.

The above described identification method resembles a *physical unclonable function (PUF) with an analogue response*. On the one hand, the method exploits the physical variations due to manufacturing processes, which are unclonable. On the other hand, the identification is based on a challenge-response function (where the workloads are the challenges while the sensor measurements are the responses). In fact, there already exist some PUF schemes which exploit analog measurements (called analog-PUF) but they are designed for analog-circuits and require added circuit to generate the unclonable function. In addition, they do not directly use the analog measurement as a response, but include a final stage where a comparator is used to generate a digital response [4] or a feature of the analog waveform is extracted as the PUF response [5]. Our proposed identification method is general and applicable to a large range of devices from FPGAs to processors. It uses the embedded sensors to generate the response, therefore no hardware overhead is incurred.

III. Experimental setup

To show the feasibility of the proposed method and to perform a preliminary analysis of its efficiency, an experimental set-up was devised. For simplicity and speedy results, we have chosen to perform a first demonstration and analysis on FPGAs. In this section, the experimental setup for our proposed identification method tailored for FPGA identification is presented.

The two main FPGA manufacturers in terms of market share (Xilinx and Intel) embed a variety of sensors that are easily accessible using ad-hoc IPs. In this work, we have used 11 evaluation boards Basys3, which are based on the latest Artix-7 FPGA from Xilinx. Each FPGA includes 32.280 Logic Cells in 5200 slices, 90 DSP slices and the XADC that is the basic building block that enables analog mixed signal functionality. The XADC includes a dual 12-bit, 1 Mega sample per second (MSPS) ADC and on-chip sensors [6]. The XADC includes one temperature sensor and three power supply voltage sensors: core voltage (VCC_{INT}), auxiliary voltage (VCC_{AUX}) and the block RAM voltage (VCC_{BRAM}). The measurements of these sensors generated during the application of a specific workload will be periodically acquired by using the XADC-IP block provided by Xilinx.

To emulate the behaviour of a device containing multiple hardware functions (located in different places of the circuit) which can be activated with different workloads, we designed a circuit having multiple ring oscillators (ROs), distributed across the target FPGA. A RO comprises an odd number of inverters following a ring configuration and its output oscillates at a specific frequency depending on several factors such as number of stages, place route, hardware imperfections, operation conditions, etc. In this work, we have implemented 5-stage ROs consisting of 4 inverters and a NAND gate that will be used to enable the RO. The ROs have been manually placed in the FPGA by using relatively placed macros (RPM). More specifically, we have evenly distributed 2025 ROs, in a grid of 15x15 ROs, in 9 different zones (225 ROs/zone) of the FPGA as depicted in Figure 1. The different zones are labeled from A to I.

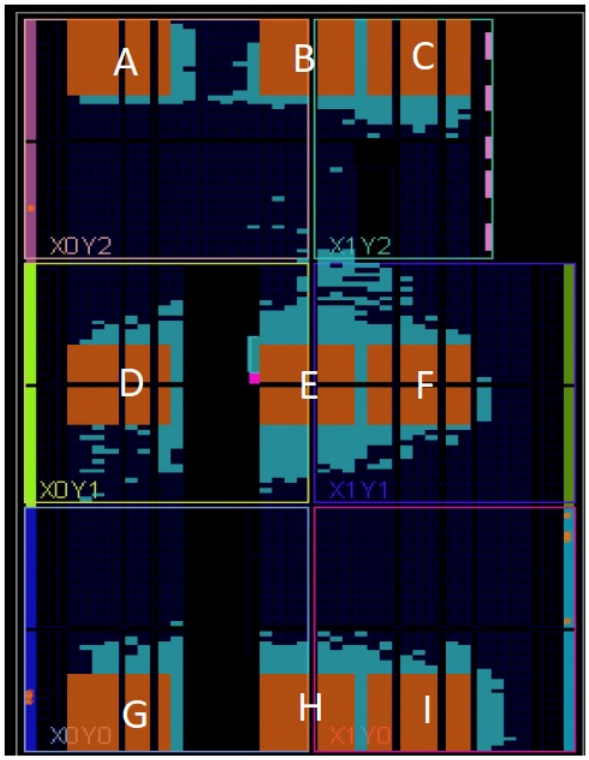

Fig. 1. 9-zone RO Distribution on the FPGA

We have created four different workloads that will be generated by turning on and off the ROs, to emulate different workloads for a real application. For completeness, the workloads have been applied at different speeds, with activation delays between consecutive ROs of 0, 10, 20, 50, and 100 ms).

- **Workload 1:** All ROs Off → Zone A→ Turn On ROs 1-by-1→ 224 ROs On→ Turn Off ROs 1-by-1→ 224 ROs Off → Next zone.
- **Workload 2:** All ROs Off → Zone A→ Turn On ROs 1-by-1→ 224 ROs On→ Next zone.
- **Workload 3:** All ROs On → Zone A→ Turn Off ROs 1-by-1→ 224 ROs Off→ Turn On ROs 1-by-1→ 224 ROs On → Next zone.
- **Workload 4:** All ROs On → Zone A→ Turn Off ROs 1-by-1→ 224 ROs Off→ Next zone.

Each of the four sensors is sampled up to 4050 times during the application of the possible workloads.

To achieve the device identification, we have used the neural network pattern recognition feature provided by Matlab 2018. It facilitates the creation of a neural network for pattern classification. We have built a neural network which correlates the sensor measurements with the physical device.

The input layer of the neural network has 16200 neurons corresponding to the number of measurement points acquired by the four sensors when a specific workload is applied. For the hidden layers, we have used a variable number of neurons that have been modified upwards from 10 to 100 neurons, setting

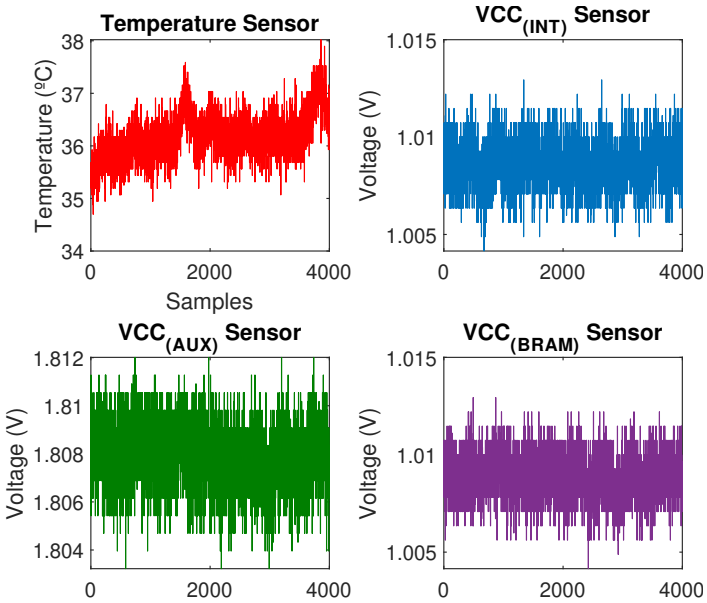

Fig. 2. Sensor responses for FPGA 1 and Workload 1

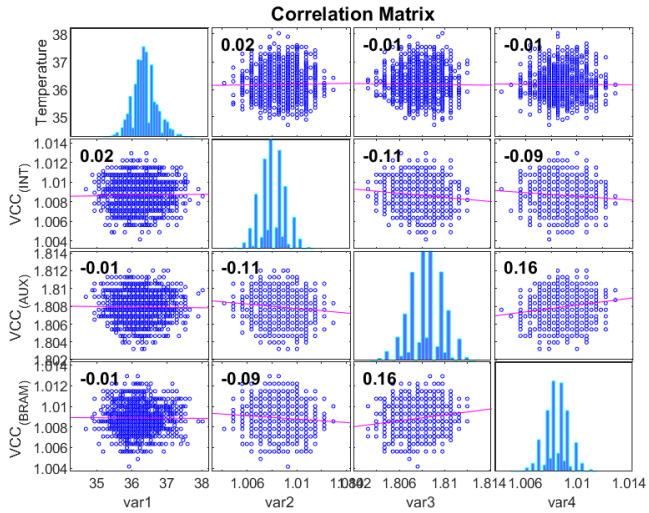

Fig. 3. Correlation matrix of sensor responses for Workload 1

a final configuration of 50-25 neurons in the hidden layers to maximize the recognition accuracy. The output layer has 11 neurons, corresponding to the number of FPGAs under analysis.

IV. Experimental Results

In this section, we present the experimental results used to evaluate the suitability of the proposed identification system.

The FPGA population to be identified is composed of 11 Artix-7 from Xilinx. We have acquired a total of 660 FPGA fingerprints corresponding to all the measurements from the on-chip sensor, under the 4 different workloads and 5 different delays, in three different days. The signatures have been generated at room temperature using always the same configuration for the power supply. In Figure 2 are depicted the measurements of the four on-chip sensors when the Workload 1 is applied. We have computed the correlation between the different sensors and depicted in Figure 3. A high positive or negative correlation means that some sensors could be removed from the configuration. In this case, there is no correlation on the sensors obtaining values close to 0.

440 FPGA signatures corresponding to two different days have been used for the training of the neural network. The rest of the signatures (220) have been used for validation purposes. Figure 4 depicts the confusion matrix for the 220 signatures (20 per FPGA) where a 99.1% of accuracy is reached in the FPGA identification. It is noteworthy that the number of observations in different classes does not vary greatly so there are no misleading results regarding the accuracy.

We have also carried out several experiments in order to evaluate the robustness of the method.

A. Sensor removal

We have removed the information of some sensors from the signature and retrained the NN using the new 440 signatures. After that, we have used a set of 220 signatures to validate

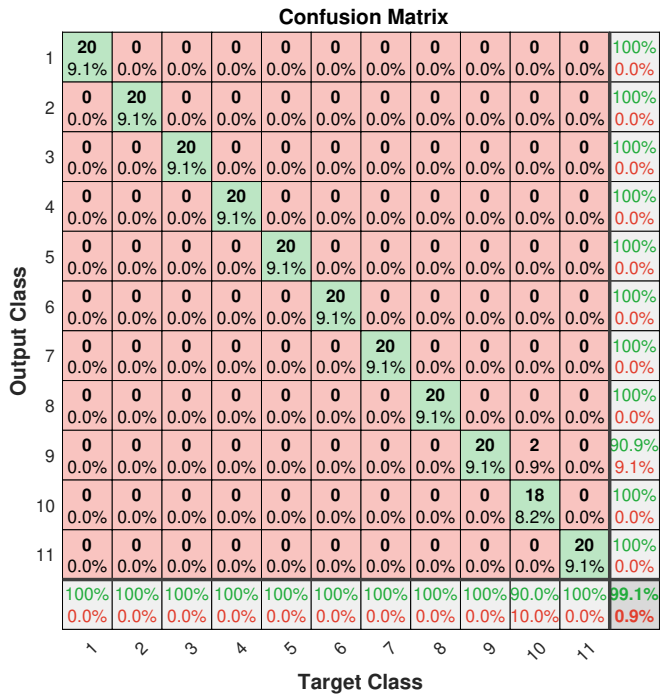

Fig. 4. Confusion Matrix for the FPGA recognition using the proposed method.

the system. In Table I are depicted the general accuracy for the different combination of sensors. It can be seen that the features extracted from the VCC_{AUX} are the most important for the identification. Nevertheless, it is shown that the combination of all sensors is necessary to obtain enough accuracy on the identification.

B. Workload removal

In this experiment, we have removed one of the workloads during the training of the NN, and then we have tried to identify the FPGAs by using the excluded patterns. The average identification accuracy obtained in this experiment is 39 % with

TABLE I
ACCURACY RESULTS FOR DIFFERENT SENSOR CONFIGURATIONS

Temperature	VCC_{INT}	VCC_{AUX}	VCC_{BRAM}	Accuracy (%)
✓	✓	✓	✓	99.1
✗	✓	✓	✓	77.7
✓	✗	✓	✓	90.9
✓	✓	✗	✓	16.8
✓	✓	✓	✗	53.2
✗	✗	✓	✓	43.2
✗	✓	✗	✓	35.0
✗	✓	✓	✗	72.7
✓	✗	✗	✓	26.8
✓	✗	✓	✗	62.7
✓	✓	✗	✗	59.1
✓	✗	✗	✗	14.5
✗	✓	✗	✗	55.5
✗	✗	✓	✗	65.0
✗	✗	✗	✓	45.0

an identification accuracy maximum of 67.3 % for workload 4. It is important to remark that the different workloads are not quite different between themselves so the identification accuracy could be even worse for workloads with more differences. These preliminary results show how difficult is to model the system and opens the doors to exploit this feature as an interesting countermeasure against some attacks that will be explained in the discussion section.

C. Delay removal

In this experiment, we have evaluated the impact of removing some delays from the training of the NN and then try to identify those workloads that have been removed. In general, the result of removing each of the delays from the training has a small impact on the identification accuracy obtaining an average result on the identification accuracy of 90%. These preliminary results indicate that the delays do not play a key role during the identification. Nevertheless, further analysis should be carried out to determine the impact of this feature on the fingerprinting of the devices.

V. DISCUSSION FUTURE WORK

The preliminary experimental results presented in the previous section are very promising. Nevertheless, some issues are still open, in particular:

- **Scalability of the system:** if the population of devices is increased to a thousand of them, with the previous results, we cannot conclude that there is a unique fingerprint for each device. Experiments shall be performed on thousands of devices in order to study the suitability of the identification method for a large device population. These new experiments will include not only more devices but also will explore a wider range of switching patterns and new architectures for the NN that could improve the identification accuracy.
- **Versatility:** the experimental setup uses ad-hoc elements (i.e., ROs) to generate different workloads, and to emulate real circuit behavior. Future research will also include the adaptation of the proposed identification to other platforms, such as microprocessors or GPUs, by activating elements existing in the system (e.g., use of an AES module to generate different switching activities).
- **Operating conditions and aging:** the results have shown the effectiveness of the proposed identification method at room temperature and normal operating conditions. It is necessary to conduct further experiments using different workloads and operating conditions. As we have access to the information of the sensors, we will normalize the measurements taking into account the initial operating conditions (voltage and temperature) in order to reduce the complexity of the training and facilitate the identification. Aging of different elements could be modeled in order to take into account their effects on the identification. Other solutions could include the retraining of the NN during the lifetime of the different devices.
- **Security:** from this perspective, the main question to be answered is related to the clonability of the system. In other words, is it possible to impersonate a legitimate device and replicate their outputs? At a first glance, the proposed system seems to be secure. Indeed, we have stated the difficulty of modeling the behavior of the entire system due to its complexity. Moreover, the unlimited number of possible workloads that can be applied makes very difficult for an adversary to predict all sensor measurements. In addition, the preliminary results presented on the subsection *Workload removal* are very promising because according to these results, the workload used to the identification must be used during the training. Thus, it will be quite difficult for an adversary to produce the correct response in an identification system where the server asks for the response of a specific workload. Other future lines could include the use of masks that select a subset of measurement points, unknowns for the adversary, for the identification. This idea is based on the fact that it is easier to obtain a higher average accuracy when replicating a large number of points than a subset of them.

REFERENCES

[1] Shanquan Tian, Wenjie Xiong, Ilias Giechaskiel, Kasper Rasmussen, and Jakub Szefer. Fingerprinting cloud fpga infrastructures. In *The 2020 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays*, FPGA '20, page 58–64, New York, NY, USA, 2020. Association for Computing Machinery.

[2] Thomas Hupperich, Henry Hosseini, and Thorsten Holz. Leveraging sensor fingerprinting for mobile device authentication. In Juan Caballero, Urko Zurutuza, and Ricardo J. Rodríguez, editors, *Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 377–396, Cham, 2016. Springer International Publishing.

[3] Hristo Bojinov, Yan Michalevsky, Gabi Nakibly, and Dan Boneh. Mobile device identification via sensor fingerprinting. *CoRR*, abs/1408.1416, 2014.

[4] L. Zimmermann, A. Scholz, M. B. Tahoori, J. Aghassi-Hagmann, and A. Sikora. Design and evaluation of a printed analog-based differential physical unclonable function. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 27(11):2498–2510, 2019.

[5] S. Deyati, B. Muldrey, A. Singh, and A. Chatterjee. Design of efficient analog physically unclonable functions using alternative test principles. In *2017 International Mixed Signals Testing Workshop (IMSTW)*, pages 1–4, 2017.

[6] Xilinx. 7 Series FPGAs and Zynq-7000 SoC XADC Dual 12-Bit 1 MSPS Analog-to-Digital Converter. *XADC User Guide UG480*, v1.10.1, 2018.