Transient Effect Ring Oscillators Leak Too

Ugo Mureddu, Brice Colombier, Nathalie Bochard, Lilian Bossuet,
Viktor Fischer

Univ Lyon, UJM-Saint-Etienne, CNRS, Laboratoire Hubert Curien UMR 5516,
F-42023, SAINT-ETIENNE, France
{ugo.mureddu, b.colombier, nathalie.bochard,
lilian.bossuet, fischer}@univ-st-etienne.fr

Abstract. Up to now, the transient effect ring oscillator (TERO) seemed to be a better building block for PUFs than a standard ring oscillator, since it was thought to be immune to electromagnetic analysis. Here, we report for the first time that TERO PUFs are in fact vulnerable to electromagnetic analysis too. First, we propose a spectral model of a TERO cell output, showing how to fit it to experimental data obtained with the help of a spectrum analyser to recover the number of oscillations of a TERO cell. We then extend it to two TERO cells oscillating simultaneously, and show how this ability can be used to fully clone a TERO PUF. These results should help designers to better plan for susceptibility of TERO PUFs to electromagnetic analysis in their future designs.

Keywords: Transient effect ring oscillator, electromagnetic leaks, side-channel analysis, semi-invasive passive attack, physical unclonable function

1 Introduction

With the sharp increase in the deployment and integration of the Internet of Things, one challenge is to ensure security with respect to privacy and trust issues. With billions of connected devices, there is a huge risk of unauthorised use or abuse. To protect from such risks, security mechanisms are needed for per-device authentication and authorisation, integrated in early design stages.

On the other hand, the miniaturisation of electronic devices is causing industrial problems since reducing the size of electronic components increases manufacturing process variability (MPV) leading, for example, to a mismatch between transistors. Although managing MPV is a challenge, silicon physical unclonable functions (PUF) are taking advantage of it since they exploit MPV to extract a secret and unique identifier per die, which is usually a binary string. This unique identifier enables identification, authentication and generation of a secret keys in many applications, including the Internet of Things [4].

For these reasons, PUFs have been a hot topic in the last decade. Since the first introduction of a PUF by Pappu in 2002 [15], many PUF principles have been published and implemented on both FPGA and ASIC. The best-known are memory-based PUFs including SRAM PUFs [17] and delay PUFs such as arbiter PUFs [18] and ring oscillator (RO) PUFs [6]. Regardless of the principle, an efficient PUF should provide an identifier per die that is unique, unpredictable, stable over time and insensitive to environmental conditions.

Among PUF principles, architectures that make use of oscillating elements were shown to be best suited for FPGA implementations [8,14].

However, it has been demonstrated that, once implemented in a physical device, PUFs are, in fact, sensitive to side channel analysis [13]. Side channel analysis refers to any attack based on information gained from a physical implementation, rather than weaknesses in the mathematical concept itself. Among the most notorious side channels are timing information, power consumption and electromagnetic leaks. In the case of RO, electromagnetic analysis is very efficient. Indeed, many studies have dealt with electromagnetic analysis of RO, showing the ability to retrieve the oscillation frequency of the ROs used for PUF or TRNG applications [12,11,1]. At the same time, a PUF architecture based on a new oscillating element emerged: the transient effect ring oscillator (TERO)-based PUF. It is supposed to be insensitive to electromagnetic analysis since it does not exploit the oscillation frequency but the number of oscillations instead [2].

In this article, we show for the first time that TERO PUFs are sensitive to electromagnetic analysis. We first demonstrate that it is possible to retrieve the number of oscillations of one TERO cell using electromagnetic analysis. We then extend this analysis and show that we can also recover the number of oscillations of two TERO cells oscillating *simultaneously*. Finally, we describe a cloning attack on a complete TERO PUF.

The rest of this article is organised as follows. In Section 2, we recall all the necessary background information about TERO PUFs. In Section 3, we present a spectral model of the TERO output. In Section 4, we provide experimental results of the EM analysis of one TERO cell, two TERO cells oscillating simultaneously, and a complete TERO PUF. Finally, Section 5 concludes this article. All VHDL design files of the FPGA implementations are available online[1] for reproducibility.

2 The transient effect ring oscillator PUF

2.1 Transient Effect Ring Oscillator

A TERO, shown in Figure 1 is a multi-event oscillating ring with signal collisions [5]. It has two states: one oscillating transient state and one non-oscillating steady state. It is composed of two branches of an odd number of inverters (delay gates) and two AND gates as activation gates. A TERO corresponds to a specific configuration of an RS latch [16].

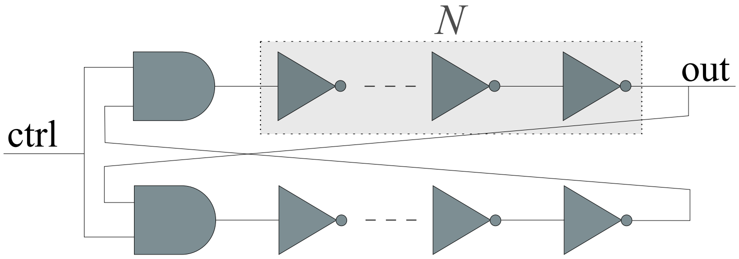


Fig. 1: A transient effect ring oscillator

When the control signal, denoted (*ctrl* in Figure 1), switches from logic level '0' to logic level '1', two electrical events start to propagate across the ring. Due to mismatches caused by MPVs between the CMOS transistors composing the ring, one event is faster than the other. That is the reason why, while the output oscillation frequency remains constant, the duty cycle drops to 0 % or rises to 100 % until the oscillations stop. Figure 2 shows an example of TERO output behaviour.

The oscillation frequency of the TERO is given in Equation (1) where d_{AND} is the mean delay of an AND gate and d_{INV} the mean delay of an inverter.

$$f_{osc} = \frac{1}{(2 \times d_{AND} + 2 \times N \times d_{INV})} \tag{1}$$

A more complete description of the TERO by Cherkaoui *et al.* can be found in [3] and by Marchand *et al.* in [10].

[1] `https://gitlab.univ-st-etienne.fr/ugo.mureddu/em-analysis-of-transient-effect-ring-oscillator-based-puf/tree/master`

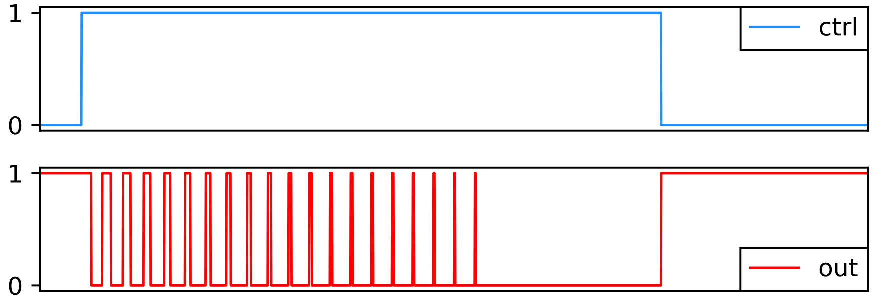


Fig. 2: TERO output behaviour (out) after activation (ctrl)

2.2 TERO PUF architecture

The TERO PUF is composed of two blocks (A and B) of m TERO cells, two n-bit counters and a bit extractor, as depicted in Figure 3. To avoid correlation, a cell in block A is always compared to a cell of the block B. One cell per block is selected using two demultiplexers. Two multiplexers then drive the correct cell output to the two n-bit counters. The cell selection signal (*select cell* in Figure 3) is usually called the challenge.

The TERO-PUF principle consists in comparing the number of oscillations of two identically implemented cells. That is why the outputs of the counters are sent to a subtractor. With this structure, 1 to 3 bits can be extracted per challenge. As explained in [9], the counters and the activation time of the control signal must be sized according to the mean number of oscillations of the TERO cells. For this study, each block is composed of $m = 128$ TERO cells with $N = 7$ inverters per branch. Counters are 11-bit wide ($n = 11$) and the activation time is set to 10 µs. Interested readers can refer to [3] for TERO cells design guidelines.

3 Spectral model of a TERO output

According to the description of the previous section, the TERO output signal is modeled to evaluate how the number of oscillations influences the spectrum amplitude. This signal is modeled as a case of pulse width modulation (PWM). This modulation technique controls the pulse duration according to a modulator signal. In the case of a TERO, the output duty-cycle increases or decreases exponentially. As a consequence, the modulator signal mod(t) is defined in Equation (2).

$$\mathrm{mod}(t) = 1 - e^{-t/\tau} \tag{2}$$

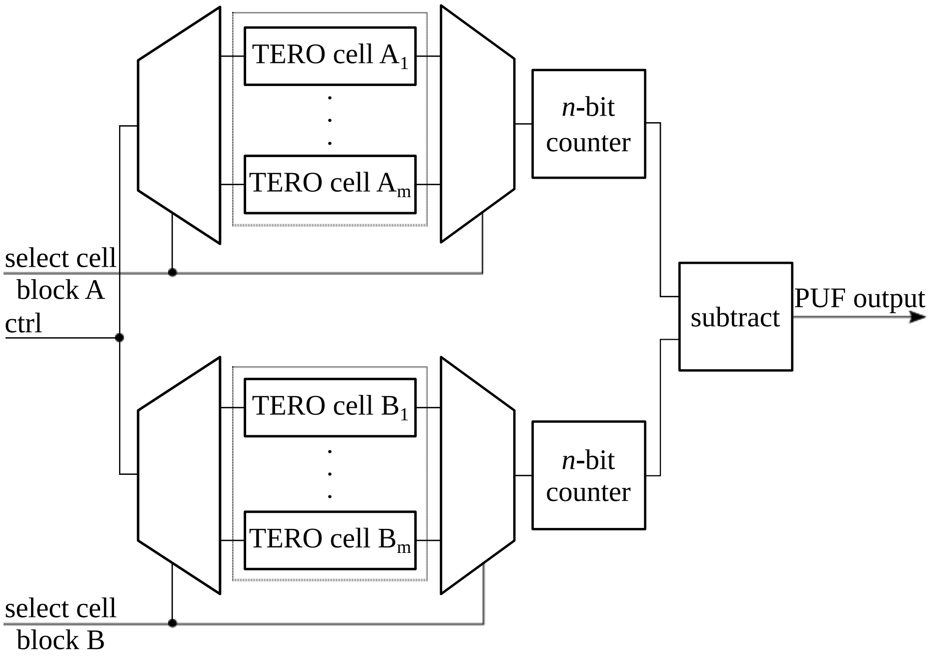


Fig. 3: TERO PUF architecture

The PWM signal ($PWM(t)$) results from the comparison of a periodic triangular signal ($\text{tri}(t)$) and $\text{mod}(t)$. Figure 4 shows the PWM signal generated when an exponential is used as a modulator signal. This behaviour was modeled and the source code is provided on the dedicated web site[2]. The smaller the τ value, the smaller the number of oscillations.

Figures 5a and 5b show the influence of the number of oscillations N_{osc} on the spectrum amplitude for $\tau = 0.1$ and $\tau = 2$. The control signal (ctrl) is modeled as a square signal with a period of 4 s, the TERO output signal (out) is modeled with $PWM(t)$ and the single-sided amplitude spectrum of the TERO output signal ($|FFTout(f)|$) is obtained with the fast Fourier transform of $PWM(t)$. The triangle wave frequency is set to 100 Hz so $f_{osc} = 100$ Hz. For $\tau = 0.1$, $N_{osc} = 9$. For $\tau = 2$, $N_{osc} = 183$.

These simulations show the impact of the number of oscillations on the spectral contribution. Namely, it highlights the fact that the spectrum of the TERO output is directly influenced by the number of oscillations. Indeed, the greater the number of oscillations, the narrower the peak at the oscillation frequency $|FFTout(f_{osc})|$. Therefore, by observing the

[2] `https://gitlab.univ-st-etienne.fr/ugo.mureddu/em-analysis-of-transient-effect-ring-oscillator-based-puf/tree/master`

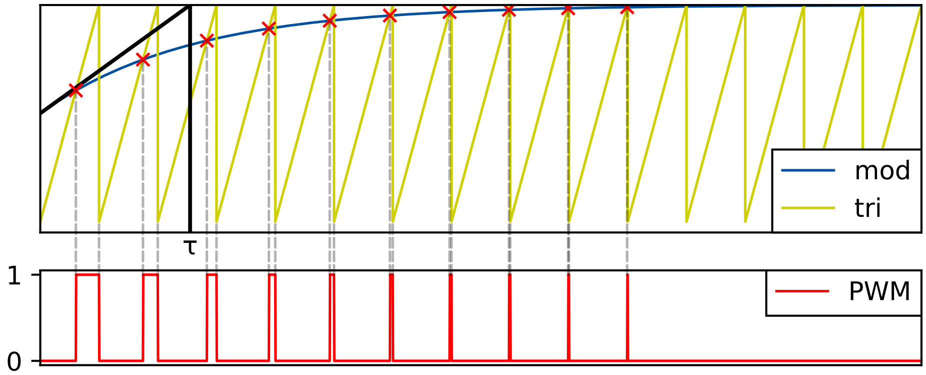


Fig. 4: TERO output model with PWM

electromagnetic emanation of a TERO cell, one can recover the number of oscillations of this cell. Since the number of oscillations is used directly to generate the PUF response, then this response can be recovered. This is demonstrated experimentally in the next section.

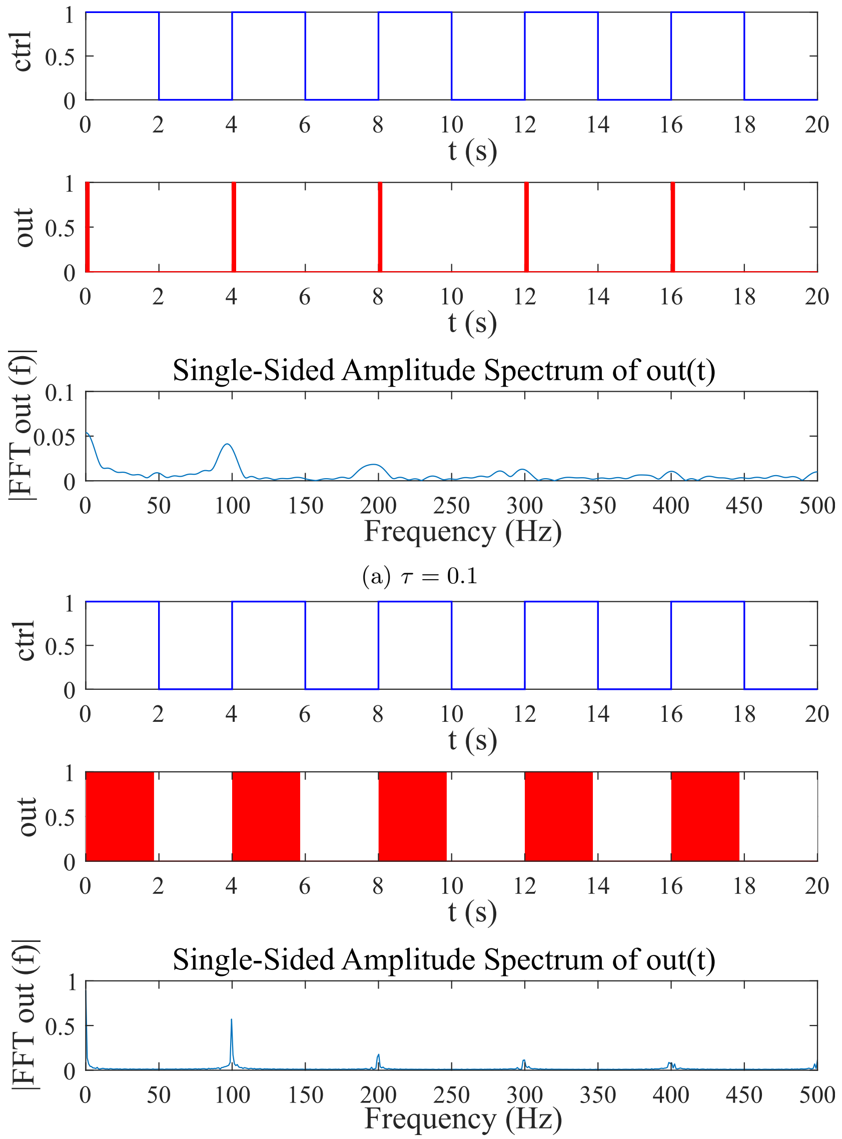
4 Passive electromagnetic semi invasive attacks

4.1 Experimental setup

The TERO electromagnetic emissions are evaluated using the setup shown in Figure 6. This setup includes:

- **An FPGA evaluation platform** called HECTOR [7] comprising a common motherboard for communication and multiple daughterboards with different FPGAs,
- **An EM probe** RS H 2.5-2 by Rohde & Schwartz,
- **A low-noise amplifier** (LNA) HZ-16 by Rohde & Schwartz connecting the probe to the spectrum analyser for measurement of high-frequency fields up to 3 GHz,
- **A real-time spectrum analyser** RSA607a by Tektronix,
- **A XYZ table** with a precision of 1 µm where the FPGA platform is fixed to move precisely under the probe,
- **A PC** to program the FPGA, control the XYZ table and record data from the spectrum analyser.

This study was performed on two FPGA families from two different manufacturers: Xilinx Spartan 6 and Intel Cyclone V to demonstrate that the results do not depend on the FPGA target. Before giving the



(a) $\tau = 0.1$

(b) $\tau = 2$

Fig. 5: TERO output FFTs for two different τ values

results of electromagnetic analysis, we detail the implementation of all the evaluated designs.

4.2 Design implementations

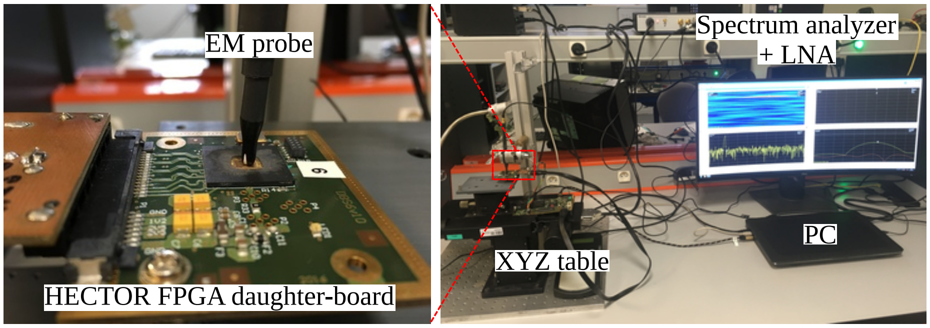
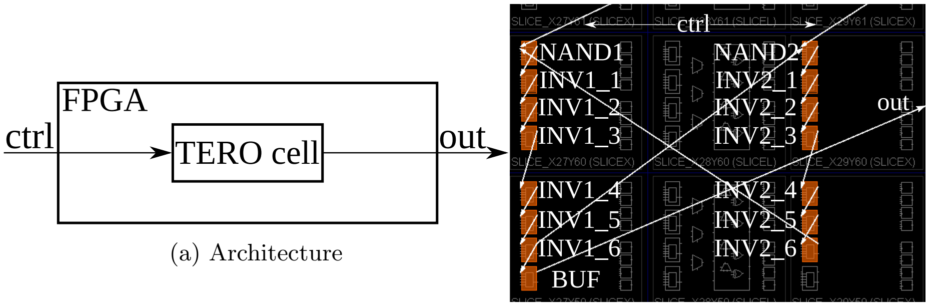


Fig. 6: Picture of the experimental setup

Design 1 - One TERO cell In this design, the FPGA is a Xilinx Spartan 6. It is configured with one $N = 7$ TERO cell. For the preliminary test, the output of the TERO cell is sent out to the oscilloscope. The TERO cell is periodically restarted by a 50 kHz control signal. Figure 7a shows the design architecture. Figure 7b shows the Xilinx ISE floor plan after implementation where each element of the TERO and their connections are visible. The output of the TERO goes through a buffer before being sent out of the FPGA.

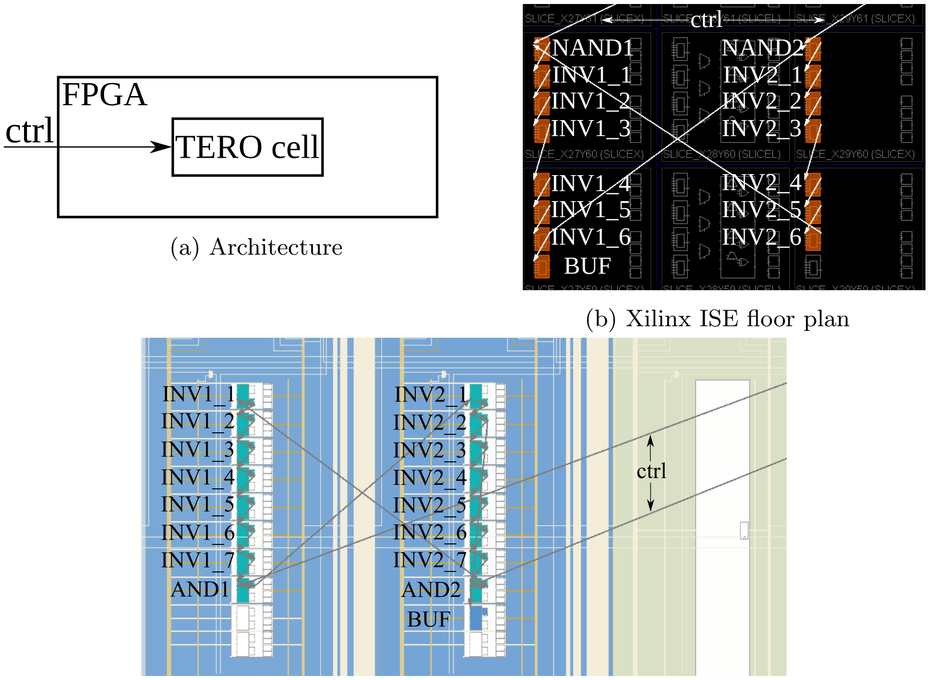


(a) Architecture

(b) Xilinx ISE floor plan

Fig. 7: Implementation of Design 1 - One TERO cell

Design 2 - One TERO cell Like in Section 4.2, only one TERO cell is implemented but the output of the cell is *not* sent out of the FPGA. This design was implemented on both Xilinx Spartan 6 and Intel Cyclone V FPGAs. Figure 8a shows the design architecture. Figure 8b and Figure 8c show screenshots of the Xilinx ISE and the Intel Quartus floor plans.



(a) Architecture

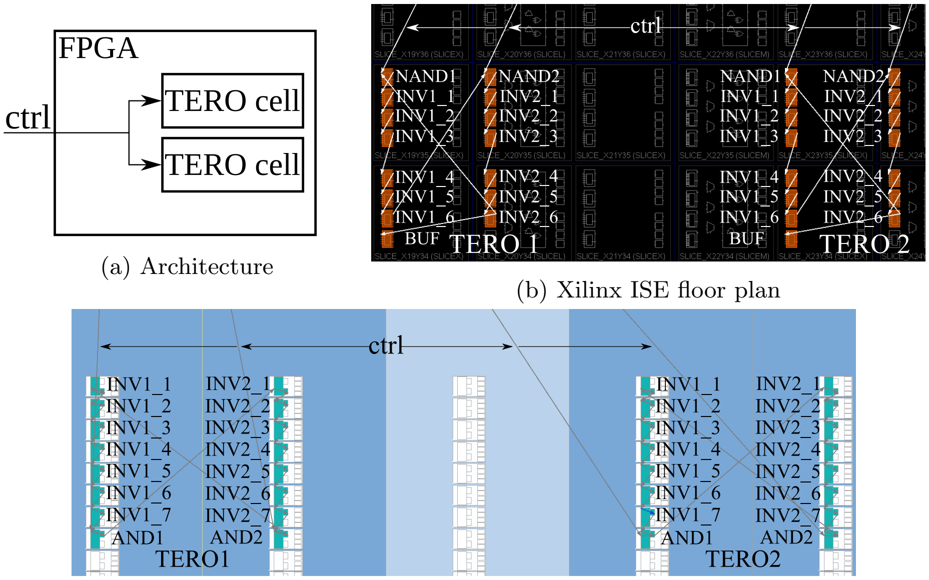
(b) Xilinx ISE floor plan

(c) Intel Quartus floor plan

Fig. 8: Implementation of Design 2 - One TERO cell

Design 3 - Two TERO cells In the third design, two TERO cells are identically implemented and activated by the same control signal. Figure 9a shows the design architecture. Figure 9b and Figure 9c show screenshots of the Xilinx ISE and the Intel Quartus floor plans. The floor plans reflect the fact that the placement of the cells are identical in both cases. This is a requirement of the PUF design to ensure that the only differences in the cells to be compared are in the MPVs.

Design 4 - TERO PUF The last design is a complete TERO PUF as described in Section 2.2, implemented on a Xilinx Spartan 6 FPGA. Figure 10a shows the design architecture. The control signal and a selection word for each block are sent to the FPGA. The PUF response and the outputs of the TERO cells are not sent out of the FPGA. Figure 10b shows a screen-shot of the Xilinx ISE floor plan after the PUF implementation where the two blocks of $m = 128$ TERO cells are clearly visible. Like for Section 4.2, TERO cells are identically implemented to extract MPVs.

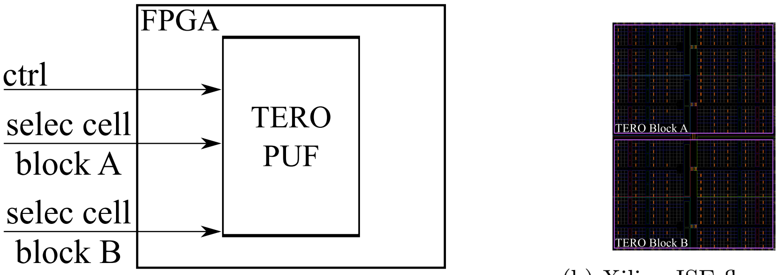


(a) Architecture

(b) Xilinx ISE floor plan

(c) Intel Quartus floor plan

Fig. 9: Implementation of Design 3 - Two TERO cells



(a) Architecture

(b) Xilinx ISE floor plan

Fig. 10: Implementation of Design 4 - TERO PUF

4.3 Electromagnetic analysis

Design 1 - One TERO cell As explained in Section 4.2, only one $N = 7$ TERO cell is implemented on a Xilinx Spartan 6 FPGA with a periodic control signal to automatically restart the TERO cell. A mean oscillation frequency of 174.4 MHz and a mean number of oscillations of 228 are recorded with the oscilloscope. Figure 11 shows the TERO oscillations observed from the oscilloscope.

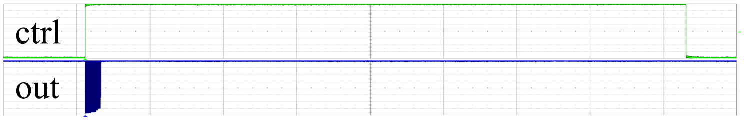


Fig. 11: TERO cell input and output observed on an oscilloscope

Since the oscillation frequency of the TERO is known, the spectrum analyser is centered at this frequency with a span of 7 MHz. By probing the FPGA, it is possible to capture the electromagnetic emissions of the running TERO cell. Figure 12 shows the results from the spectrum analyser.

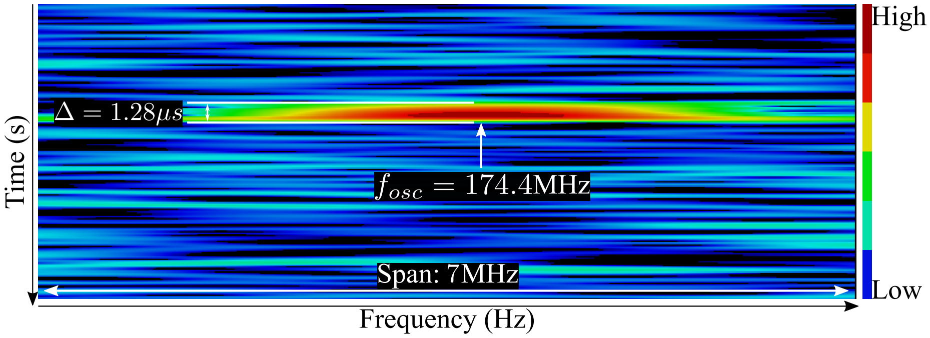


Fig. 12: Spectrogram of one TERO cell EM emanation

The spectrogram gives the emission amplitude (red represents high amplitude and blue low amplitude) per frequency over time. In Figure 12, the oscillation frequency of the TERO can be seen clearly at 174.4 MHz. It is also possible to retrieve for how long it oscillates. In this case, it oscillates for 1.28 µs. With the oscillation frequency and the duration of oscillation, the number of oscillations can be computed: $N_{osc} = 1.28 \times 10^{-6} \times 174.4 \times 10^{6} = 223$. It is worth noting that there is a slight difference between the number of oscillations computed with the electromagnetic emission and the one measured with the oscilloscope. This is because the oscilloscope records a mean of all the TERO runs whereas the spectrum analyser records only one run in real time. Once the oscillation frequency of the TERO is identified, another representation of the electromagnetic emissions provided by the spectrum analyser can be used: amplitude versus time (see Figure 13). This allows for an easy measurement of the duration of oscillation. Figure 13 shows that spectrum amplitude increases with time, *i.e.* with the number of oscillations. This confirms that a passive attacker can recover the number of oscillations of one TERO cell, in accordance with the simulations described in Section 3.

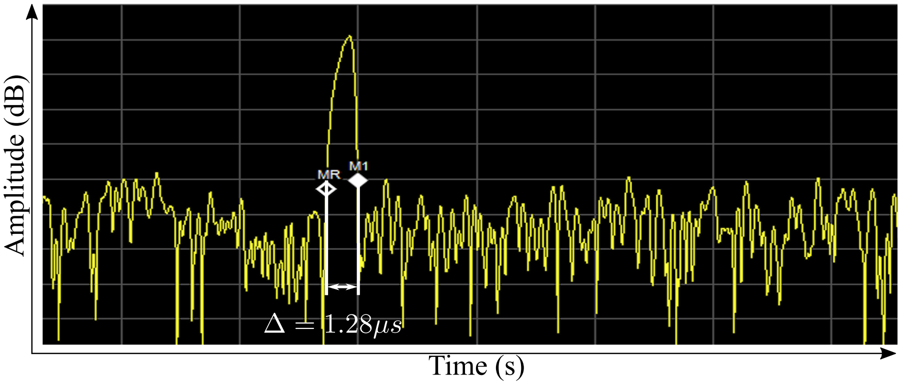


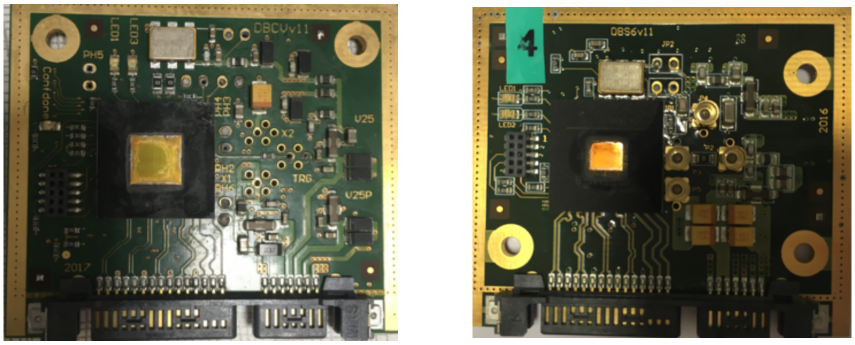
Fig. 13: Amplitude vs time of one TERO cell EM emanation at 174.4 MHz

Design 2 - One TERO cell Following the approach detailed in [1], we performed a mapping of the electromagnetic emanation of the FPGA at 174.4 MHz without outputting the TERO output signal. Unfortunately, this does not lead to a successful identification of any electromagnetic emission. Indeed, the TERO emission is not powerful enough to emerge from the ambient electromagnetic noise. In the first experiment, this simple approach was successful because sending the signal to an output of the FPGA increased the emission amplitude. The analysis of a TERO cell implemented on an Intel Cyclone V FPGA lead to similar results.

In contrast with RO electromagnetic analysis, since the TERO only oscillates for a limited period of time, it does not radiate sufficiently to be captured by the spectrum analyser without sending its signal on an output of the FPGA. To analyse the TERO output signal without sending it out of the FPGA, decapsulation is required.

For this reason, in the following experiments, we decapsulated the FPGAs before electromagnetic analysis. The decapsulation protocol is the same as described in [19]. Figure 14 shows the two decapsulated FPGAs.

After decapsulation, we performed a mapping of both FPGAs to detect the electromagnetic emission of the TERO cells. For the TERO cell



(a) Intel Cyclone V

(b) Xilinx Spartan 6

Fig. 14: Decapsulated FPGAs

implemented on Xilinx Spartan 6, the result is similar to that of experiment 1: the number of oscillations is close to 225. For the TERO cell implemented on Intel Cyclone V, we identified an oscillation frequency of 198 MHz and a number of oscillations of 462.

Design 3 - Two TERO cells For this experiment, two $N = 7$ TERO cells are implemented in the decapsulated Xilinx Spartan 6 FPGA. The TERO outputs are not sent out of the FPGA and the two TEROs are triggered simultaneously by the same control signal. Figure 15 shows the spectrogram resulting from this experiment. The electromagnetic emission captured by the spectrum analyser can be divided into two parts. In the first part, both TERO cells are running. In the second part, only one TERO cell is still running. The first part lasts for 1.28 µs during which the TERO from Section 4.3 can be identified. The loss of amplitude after 1.28 µs makes it possible to identify that one TERO cell stops oscillating. It is also important to note that during the first part, the electromagnetic emission span is larger. Indeed, the two TEROs do not oscillate at the exact same frequency. This is a second hint that one TERO cell stopped oscillating. From this experiment, the two TERO cells and their number of oscillations can be identified undoubtedly. The first TERO cell oscillates 223 times at 174.4 MHz. The second TERO cell oscillated at 174.6 MHz for 5.11 µs. Thus, the number of oscillations of the second TERO cell is 892.

This experiment shows that even when two TERO cells are started simultaneously, their respective number of oscillations can be recovered successfully.

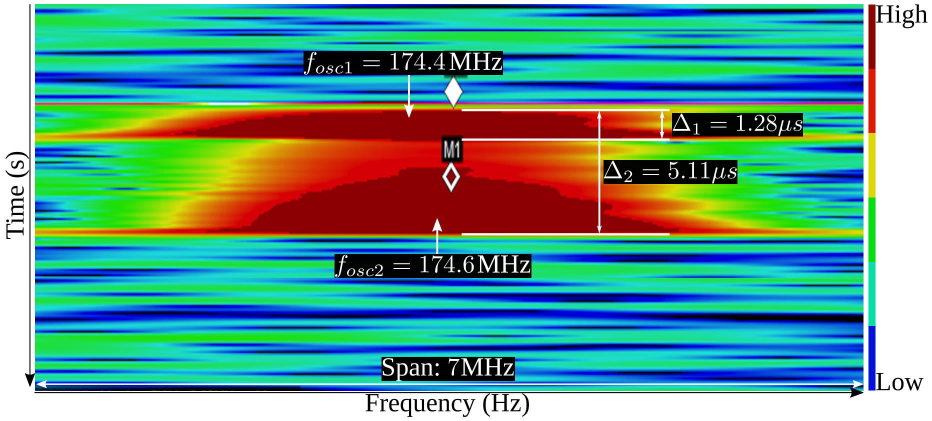


Fig. 15: Spectrogram of the EM emanation of two TERO cells

Design 4 - TERO PUF Since we demonstrated that it is possible to retrieve the number of oscillations of two TERO cells oscillating at the same time, the experiment was done on the PUF described in Section 4.2. It should be recalled that TERO cells composing the PUF are implemented identically with $N = 7$ delay elements. Implementation details are available in [9]. For this reason, all TERO cells oscillate at around 174 MHz. Thus, the spectrum analyser is centered at 174 MHz with a span of 7 MHz to make sure that we capture the spectrum of all the TERO cells when they oscillate.

As mentioned in 2.2, the activation time of the TERO cells for each comparison is 10 µs. Figure 16 shows the spectrogram of four successive comparisons of TERO cells from block A with TERO cells from block B. Dividing Figure 16 vertically in blocks of 10 µs allows to isolate each comparison. For this experiment, successive comparisons are as follows: TERO cell A_i is compared with TERO cell B_i, TERO cell A_{i+1} is compared with B_{i+1} and so on. This proves that the spectrum analyser can catch successive TERO runs.

For obvious security reasons, the result of the comparison of the two TERO cells is not sent out of the FPGA directly. However, assuming that users have access to the PUF challenge, only a small number of comparisons combined with electromagnetic analysis are sufficient to clone the PUF.

First, the comparisons of the (A_1, B_1) and (A_1, B_2) pairs allow to retrieve the number of oscillations of A_1 by finding the common pattern in both comparisons. Second, the comparisons of the (A_1, B_i) pairs are per-

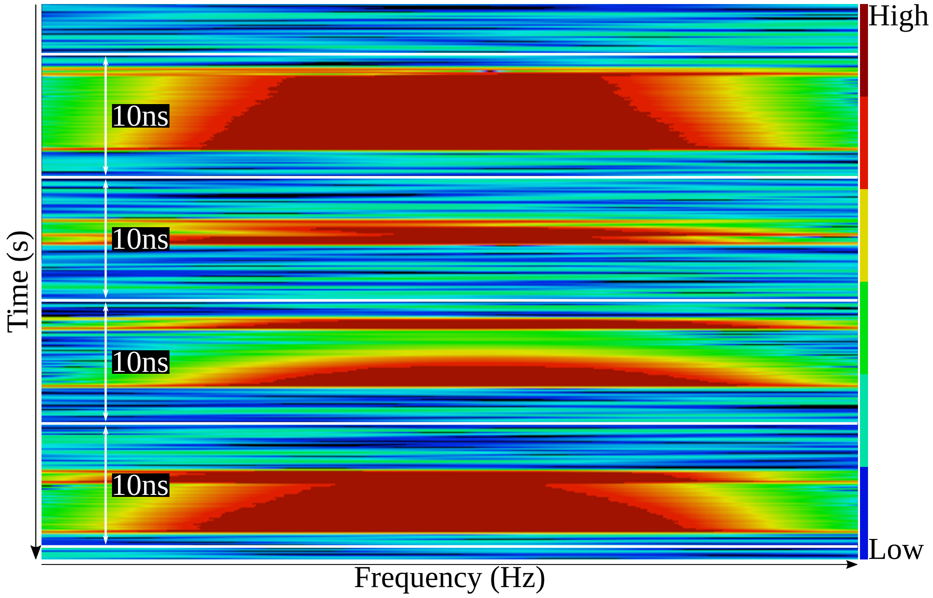


Fig. 16: Spectrogram of the EM emanation of a TERO PUF

formed for i ranging from 3 to m. This reveals the number of oscillations of all the TERO cells in block B. Third, the comparisons of the $(A_i,\, B_1)$ pairs are performed for i ranging from 2 to m. This reveals the number of oscillations of all the TERO cells in block A. Eventually, $2 \times m - 1$ comparisons are sufficient to retrieve the number of oscillations of all the cells and clone the PUF.

5 Conclusion

In this article, we presented and discussed electromagnetic analysis of TERO PUFs. We show for the first time that TERO cells leak and that consequently, their number of oscillations can be retrieved without accessing their outputs. This gives the ability to fully clone a TERO PUF. By performing the study on two FPGAs made by two different manufacturers, we also demonstrated that electromagnetic analysis is efficient whatever the device used. It is important to note that outputting the TERO signal on an FPGA output increases the electromagnetic emission. What is more, it is free access to the challenges of the PUF that makes it possible to clone it. The results presented here, together with the freely available VHDL codes, will help designers to better foresee and prevent TERO leakages in their future designs.

Acknowledgements

This work was carried out in the framework of the FUIAAP22-Project PILAS supported by Bpifrance.

References

1. P. Bayon, L. Bossuet, A. Aubert, and V. Fischer. Electromagnetic analysis on ring oscillator-based true random number generators. In *International Symposium on Circuits and Systems*, pages 1954–1957, 2013.
2. Lilian Bossuet, Xuan Thuy Ngo, Zouha Cherif, and Viktor Fischer. A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon. *IEEE Transactions on Emerging Topics in Computing*, 2(1):30–36, 2014.
3. 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*, 11(6):1291–1305, June 2016.
4. Abdelkarim Cherkaoui, Lilian Bossuet, Ludwig Seitz, Göran Selander, and R. Borgaonkar. New paradigms for access control in constrained environments. In *International Symposium on Reconfigurable and Communication-Centric Systems-on-Chip*, pages 1–4, Montpellier, France, May 26-28 2014.
5. Viktor Fischer, Patrick Haddad, and Abdelkarim Cherkaoui. Ring oscillators and self-timed rings in true random number generators. In Yoshifumi Nishio, editor, *Oscillator Circuits: Frontiers in Design, Analysis and Applications*, pages 267–292. IET, 2016.
6. Blaise Gassend, Dwaine Clarke, Marten van Dijk, and Srinivas Devadas. Silicon physical random functions. In *Conference on Computer and Communications Security*, CCS '02, pages 148–160, New York, NY, USA, 2002. ACM.
7. M. Laban, M. Drutarovsky, V. Fischer, and M. Varchola. Modular evaluation platform for evaluation and testing of physically unclonable functions. In *International Conference Radioelektronika*, pages 1–6, April 2018.
8. Abhranil Maiti, Jeff Casarona, Luke McHale, and Patrick Schaumont. A large scale characterization of RO-PUF. In *International Symposium on Hardware-Oriented Security and Trust*, pages 94–99, Anaheim Convention Center, California, USA, 13-14 June 2010. IEEE.
9. C. Marchand, L. Bossuet, and A. Cherkaoui. Design and characterization of the TERO-PUF on SRAM FPGAs. In *Annual Symposium on VLSI*, pages 134–139. IEEE Computer Society, July 2016.
10. C. Marchand, L. Bossuet, U. Mureddu, N. Bochard, A. Cherkaoui, and V. Fischer. Implementation and characterization of a physical unclonable function for IoT: A case study with the TERO-PUF. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 37(1):97–109, Jan 2018.
11. D. Merli, J. Heyszl, B. Heinz, D. Schuster, F. Stumpf, and G. Sigl. Localized electromagnetic analysis of RO PUFs. In *International Symposium on Hardware-Oriented Security and Trust*, pages 19–24. IEEE, June 2013.
12. Dominik Merli, Dieter Schuster, Frederic Stumpf, and Georg Sigl. Semi-invasive EM attack on FPGA RO PUFs and countermeasures. In *Workshop on Embedded Systems Security*, WESS '11, pages 2:1–2:9, New York, NY, USA, 2011. ACM.

13. Dominik Merli, Dieter Schuster, Frederic Stumpf, and Georg Sigl. Side-channel analysis of PUFs and fuzzy extractors. In JonathanM. McCune, Boris Balacheff, Adrian Perrig, Ahmad-Reza Sadeghi, Angela Sasse, and Yolanta Beres, editors, *Trust and Trustworthy Computing*, volume 6740 of *Lecture Notes in Computer Science*, pages 33–47. Springer Berlin Heidelberg, 2011.
14. Sergey Morozov, Abhranil Maiti, and Patrick Schaumont. An analysis of delay based PUF implementations on FPGA. In Phaophak Sirisuk, Fearghal Morgan, Tarek El-Ghazawi, and Hideharu Amano, editors, *Reconfigurable Computing: Architectures, Tools and Applications: 6th International Symposium, ARC*, pages 382–387, Bangkok, Thailand, March 2010. Springer Berlin Heidelberg.
15. Ravikanth Pappu, Ben Recht, Jason Taylor, and Neil Gershenfeld. Physical one-way functions. *Science*, 297(5589):2026–2030, 2002.
16. L. M. Reyneri, D. Del Corso, and B. Sacco. Oscillatory metastability in homogeneous and inhomogeneous flip-flops. *IEEE Journal of Solid-State Circuits*, 25(1):254–264, Feb 1990.
17. Ying Su, J. Holleman, and B.P. Otis. A digital 1.6 pJ/bit chip identification circuit using process variations. *IEEE Journal of Solid-State Circuits*, 43(1):69–77, Jan 2008.
18. G. Edward Suh and Srinivas Devadas. Physical unclonable functions for device authentication and secret key generation. In *Design Automation Conference*, pages 9–14, San Diego, CA, USA, June 4-8 2007.
19. Christian Wittke, Zoya Dyka, Oliver Skibitzki, and Peter Langendoerfer. Preparation of SCA attacks: Successfully decapsulating BGA packages. In Ion Bica and Reza Reyhanitabar, editors, *Innovative Security Solutions for Information Technology and Communications*, pages 240–247. Springer International Publishing, 2016.