Modeling Thermal Effects For Biasing PUFs

Aghiles Douadi, Ioana Vatajelu, Paolo Maistri, David Hély, Vincent Beroulle, Giorgio Di Natale

Modeling Thermal Effects For Biasing PUFs

Aghiles Douadi*, Elena-Ioana Vatajelu*, Paolo Maistri*, David Hely†, Vincent Beroulle† and Giorgio Di Natale*
*Univ. Grenoble Alpes, CNRS, Grenoble INP[1], TIMA, 38000 Grenoble, France
†Univ. Grenoble Alpes, Grenoble INP[1], LCIS, 26000 Valence, France

***Abstract*—Security primitives such as Physical Unclonable Functions (PUFs) or True Random Number Generators (TRNGs), have emerged as hardware roots of trust for ensuring the security of modern applications. However, these primitives display susceptibility to physical attacks, among them, in the face of temperature variations. Previous research has established the feasibility of attacks exploiting temperature fluctuations to compromise the security of these primitives. Specifically, when implemented on FPGAs, programmable components can be vulnerable to alterations induced by thermal changes. These findings underscore the need to deepen the understanding of the implications of temperature sensitivity on the security and robustness of these security mechanisms. This paper studies how heat affects, both instantaneously and permanently, the working of ring oscillators, which are the building blocks of PUFs based on Ring Oscillators. The study also suggests how to exploit these effects to bias the PUf responses, enabling thus the possibility of its cloning.**

I. Introduction

Hardware attacks encompass various types, including invasive, semi-invasive, and non-invasive attacks [1]. Several attack techniques exist, such as clock glitches, electromagnetic attacks (EM), laser attacks, X-rays, voltage alterations, and temperature-based attacks [2]. They can occur in two ways: either to induce dynamic misbehaviour when the circuit is powered on and an operation is being executed, or to introduce a permanent effects to bias electrical or physical characteristics of some elements of the circuit.

This paper contributes to the characterization of thermal effects on a Xilinx Spartan-7 family FPGA, thanks to the implementation of a specific module designed to generate localised high temperatures. The main objective of this study is to enhance our understanding of the thermal dynamics within the FPGA chip, revealing the mechanisms of temperature propagation and highlighting thermal gradients. The study also investigates the impact of temperature on structures such as Ring-Oscillators (ROs) implemented on the FPGA, considering two essential aspects: real-time effects characterized when the thermal module is activated, and permanent effects characterized when the thermal module is turned off after a certain heating period. We focus in particular on ROs, because of their crucial role in RO-PUFs. Furthermore, this paper aims to generalize the observed thermal effects and their propagation in the FPGA to demonstrate the potential exploitation of such manipulation for tampering with the responses of a PUF.

[1]Institute of Engineering Univ. Grenoble Alpes

This work was supported by a research grant from the French Agence Nationale de la Recherche (POP project, ANR-21-CE39-0004)

This paper is organized as follows. In Section II, we offer a brief overview of the two primary effects of temperature on CMOS devices. The characterization of temperature within the FPGA and the methodology employed for this purpose are detailed in Section III. Section IV presents the results of temperature effects on ROs implemented on FPGA. An overview is provided in Section V on how these results can be applied within the context of Physical Unclonable Functions (PUFs) implemented on an Application-Specific Integrated Circuit (ASIC). Finally, Section VI concludes the paper.

II. Temperature effect on CMOS devices

This section provides an overview of the temperature effects on CMOS devices and their impact on internal parameters of transistors, such as threshold voltage, mobility, and current.

A. Real-Time Effects

In transistors, the electrical mobility and threshold voltage are two parameters directly influenced by temperature, giving rise to fluctuations in the transistor's drain saturation current. The carriers mobility $U(T)$ and threshold voltages $V_t(T)$ exhibit temperature dependence [3], which is characterized by the following equations [4]:

$$U(T) = U(T_0)\left(\frac{T}{T_0}\right)^{-UTE} \tag{1}$$

$$V_t(T) = V_t(T_0) - \sigma(T - T_0) \tag{2}$$

Where T_0 and T represent the reference temperature (300K) and the operating temperature, respectively. The variable UTE denotes the mobility temperature exponent, and σ is the threshold voltage temperature coefficient.The increase in temperature leads to a decrease in the transistor's threshold voltage and electrical mobility. Generally, the impact on mobility prevails over the effect on the threshold voltage. This has significant implications for security, where, for instance, a temperature rise reduces the drain saturation current (Eq. 3), consequently lowering the frequencies of ROs that form the foundation of RO-PUFs:

$$I_D = \frac{1}{2}\frac{W}{L}U(T)C_{OX}(V_G - V_t(T))^{\alpha} \tag{3}$$

With W = width, L = length, $U(T)$ = carriers mobility, C_{OX} = gate capacitance, V_G = gate voltage, $V_t(T)$ = threshold voltage, α velocity saturation index. This effect is transient, as transistors regain their nominal current values once the thermal stress is alleviated.

B. Permanent Effects

Higher temperatures can speed up aging processes, due to Bias Temperature Instability (BTI). Negative Bias Temperature Instability predominantly affects pMOS transistors. However, with the incorporation of high-k dielectric in sub-45 nm nodes, Positive BTI (PBTI) in nMOS transistors becomes significant and cannot be dismissed. The combination of heightened temperatures and substantial supply voltages leads to the creation of positively charged interface traps when transistors are biased in strong inversion. Over the long term, this contributes to an increase in the transistor's threshold voltage. Another phenomenon exacerbated by temperature in FPGAs is Time Dependent Dielectric Breakdown (TDDB). TDDB occurs when the voltage applied at the grid stack generates traps within the dielectric. These traps can create a conductive path through the grid dielectric, commonly referred to as oxide breakdown. Recent studies [5] [6] have demonstrated the use of these thermal effects to conduct cloning attacks on PUF. In [5], the authors detailed how real-time effects due to high temperatures reduce the standard deviation of the frequency distribution of ring oscillators (ROs). Additionally, [6] explained how permanent temperature effects influence SRAM-PUF responses due to the aging process.

III. Heat Characterization and Modeling

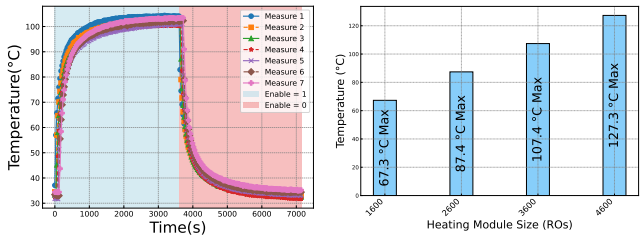
This section characterizes temperature evolution in a Xilinx Spartan-7 FPGA (xc7s25) through a dedicated heating module. Objectives include understanding heat-induced changes, analyzing module parameters, studying heat propagation, and demonstrating a temperature gradient. The method utilizes single-inverter Ring Oscillators (ROs), known as the "Heating Module," for generating substantial temperature increases in FPGAs without external equipment, working across all types. The approach involves a custom routing algorithm for optimal RO placement, considering LUT confidentiality. In FPGAs, two main sources of heat can be identified and classified as follows: static temperature, primarily caused by transistor leakage currents, and dynamic temperature. Dynamic heat is induced by cross-conduction losses and capacitive power losses due to switching activity. Dynamic Power losses (P_d) on a network can be calculated as follows:

$$P_d = CV^2 \alpha f \tag{4}$$

where C is capacitance, V is supply voltage, α is the Switching Rate and f is the switching frequency. The actual frequency of a Ring-Oscillator (RO) depends on various parameters, and its model is often complex and incomplete. A simplified formula to model the frequency is [7]:

$$Frequency = \frac{1}{2 \cdot D \cdot N} \tag{5}$$

where D is the propagation delay of each inverter, and N is the number of inverters. A Heating Module with 3600 single-inverter ROs was implemented in the FPGA. Activating the module led to a rapid temperature rise, stabilizing at 107°C after 33 minutes, as measured by the internal sensor.



(a) (b)

Fig. 1: (**a**) Evolution of the FPGA temperature caused by the Heating Module, (**b**) Maximum Temperature as a function of the Heating Module size.

Deactivation returned the FPGA temperature to its initial value in the same time frame (Figure 5a).

The observed effect is directly proportional to the size of the Heating Module used. In Figure 5b, we consistently observe a correlation between the number of the single-inverter ROs and the generated temperature. With each addition of 1000 ROs, the total generated temperature increases by +20 °C.

TABLE I: Temperature dependance on FPGA

Board	FPGA1	FPGA2	FPGA3	FPGA4	FPGA5
Temperature Max	102°C	107°C	106°C	107°C	105°C
Temperature Min	33°C	36°C	35°C	37°C	36°C

To ensure that the temperature generated by our Heating Module is reproducible on other FPGAs of the same family, we conducted tests on several FPGAs from the Spartan-7 family, implementing the same Heating Module (3600 single-inverter ROs). Table I provides an overview of the temperature behavior across different FPGAs from the same family. Although the maximum value may vary slightly, it is consistent with the margin of error; moreover, the difference between the maximum and minimum remains consistent across all FPGAs, around 70°C.

Once we understand the relationship between the parameters of the Heating Module and the induced heat, and how such heat evolves within the FPGA, our next goal is to ascertain whether there is a temperature gradient within the FPGA chip – in other words, whether the temperature is homogeneous across the FPGA. The crucial step in this study is finding the temperature sensor, undisclosed in the FPGA datasheet for confidentiality reasons. Analyzing temperature changes and identifying the maximum temperature point helped us accurately determine the sensor's location and study temperature propagation. To locate the temperature sensor, we generated seven bit-streams, each containing a "Heating Module" of 1600 single-inverter ROs placed at various locations on the chip, routed exactly in the same manner. We selected this number of ROs to achieve a measurable temperature increase across the entire FPGA surface while keeping the heater module as compact as possible.

From the findings depicted in Figure 2, it is evident that the temperature variation and the maximum rate of evolution are

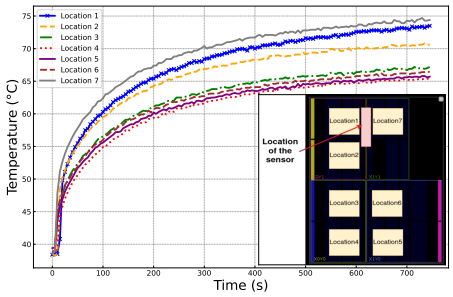


Fig. 2: Internal temperature evolution as a function of the **Heating Module** position in the FPGA chip.

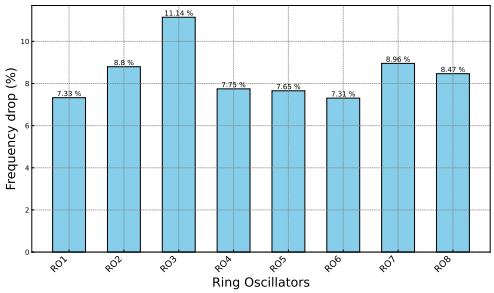


Fig. 4: Ring Oscillators' frequency variation as a consequence of temperature increase and internal voltage drop induced by the **Heating Module** in FPGA chip, measured in real-time.

contingent upon the spatial positioning of the Heater Module. When it is positioned in locations 1 and 7, at the topmost part of the chip, the temperature increases more rapidly (0.18°C per second) and reaches a maximum of 74°C after 700 seconds. Conversely, when placed in the lower regions of the chip (locations 4 and 5), the temperature evolves more slowly with a slope of 0.12°C per second, reaching a maximum temperature of 66°C. This observation leads us to infer that the temperature sensor is located at the top of the chip in the figure 4 (between locations 1 and 7). With this Heating module configuration, there is a maximum 8°C difference between the two farthest zones, demonstrating that the temperature does not propagate uniformly across the entire chip.

IV. Temperature effect on ROs frequencies

In this section, we highlight the effects of the temperature generated by the "Heating Module" on ROs implemented on an FPGA. To achieve this, we implemented 8 ROs, each comprising 103 inverters, in addition to a "Heating Module" module containing 3600 single-inverter ROs, all on a Xilinx Spartan-7 FPGA, as depicted in Figure 3. The 8 ROs will enable us to understand the thermal distribution generated by the "Heating Module" on the FPGA and its impact on ROs frequency. We begin with a real-time study of these effects, followed by an examination of their permanent implications.

A. Real-Time Effects

The purpose of this study is to understand how the ROs respond to a localized thermal attack on the FPGA.

Upon activation of the Heater Module, the temperature reaches a pick of 107°C after 33 minutes. However, alongside to the temperature change, the internal supply voltage decreases from 1V to 0.967V due to IR drop. This drop occurs when the switching activity of the transistors is high, leading to an increased current demand and subsequent voltage decrease. In Figure 4, it is shown that all the ROs experience a significant frequency drop; in particular, it is interesting to note that RO3 exhibits the most significant drop of 11.14%; on the other hand, ROs 1, 4, 5, and 6, which are the farthest from the heating source, show a smaller decrease. Additionally, we observe that RO7 and RO8, despite being in close proximity to the heater similar to RO3, experience a much smaller drop. This observation suggests that temperature propagation within the FPGA is more pronounced along the vertical axis than the horizontal axis. It is worthy to consider that, in this specific case, the frequency drop is not solely due to the temperature but also likely influenced by the overall reduction in voltage.

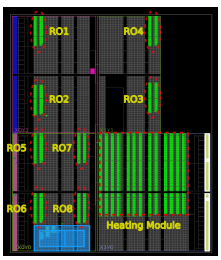
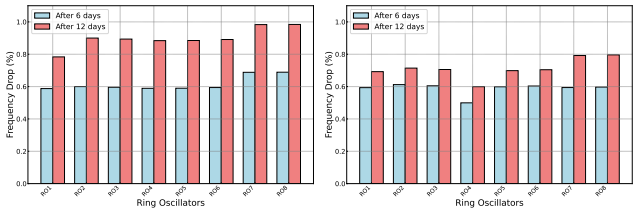


Fig. 3: Methodology to study the effect of the temperatuer generated by our module on ROs frequencies in FPGA.

B. Permanent Effects

Following the same structure as presented in Figure 3, we investigated the permanent effects of temperature on the frequencies of the ROs. In contrast to the previous "Real-Time Effects" where ring oscillator frequencies are measured while the "Heating Module" is in operation, incorporating both voltage drop and temperature effects, we followed here a different procedure. We measured the frequencies of the 8 ROs before turning on the "Heating Module". Then, we activated the "Heating Module", raising the temperature to 107°C. We kept the heating device running for several days and then turned it off. Once the FPGA had returned to its initial temperature, we conducted a new measurement of the RO frequencies. Two configurations were used: one where the ROs oscillate continuously during the heating phase (Enable = 1), and the other where the ROs do not oscillate (Enable = 0) and are activated only during measurement. Figure 5 illustrates a discernible decrease in the frequencies of all Ring Oscillators (ROs), with a notably pronounced trend observed for ROs 7 and 8, particularly when situated in proximity to the heating device. Moreover, the configuration in which ROs oscillate continuously exhibits a less pronounced frequency decrease than when the ROs are deactivated. This phenomenon can be attributed to aging effects, particularly Bias Temperature Instability. As demonstrated in [8], the effects of NBTI and PBTI are more pronounced when the ROs remain continuously



(a) Enable = 0 (b) Enable = 1

Fig. 5: Evolution of the frequencies of ring oscillators as a function of the permanent effect of temperature, (**a**) the ROs are under voltage during the heating period but do not oscillate, (**b**) the ROs oscillate continuously during the heating period.

polarized, whereas when they oscillate between the "ON" and "OFF" states, the effects are less significant due to a recovery effect.

V. Exploitation in PUF

To further assess the thermal effect, we set up a simulation environment based on the ST 65nm technology. Our goal is to better understand how the presence of a temperature gradient influences the response of a RO-PUF. Assuming laser heating allows for rapid elevation to high temperatures (within a few seconds), we hypothesize a more significant gradient under these conditions compared to the maximum gradient observed in our FPGA with the heating module. If a heat source is applied to a RO in a chip, the temperature tends to spread. Specifically, when using a thermal laser targeting a part of the chip, it can induce a very rapid temperature rise, reaching several hundred degrees. In this study, we set a limit at 200 °C to preserve the integrity of the structure. In our simulations, we assumed that the targeted RO would reach a temperature of 200 °C, and the nearest RO would have a difference of 5 °C (thus at 195 °C), propagating through the chip with a temperature decrease of 5 °C at each subsequent ring. Each RO in each subsequent ring is generated 1000 times using the Monte Carlo method to account for process variability. We use the RO at 200 °C as a **Reference RO** and compare each of the 1000 possible frequency values of this RO with the 1000 possible values of other ROs in subsequent rings. Thus, we obtain a response of 1 million bits at each temperature iteration. In Figure 6, it is observable

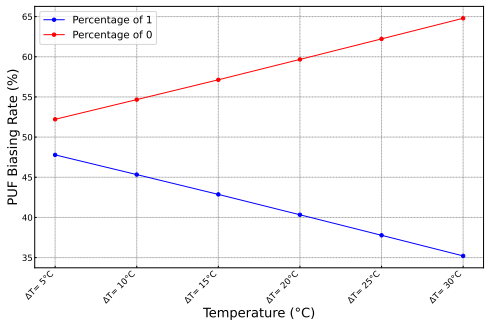


Fig. 6: Evolution of the biasing rate of the targeted RO.

that each time the temperature difference δT between the reference RO and the one it is compared to increases by 5°C, the probability of obtaining a comparison output equal to zero increases by 2%, this observation means that the reference RO has a lower frequency than the other ring, when the temperature difference δT increases. It is important to emphasize that we are transitioning from physical/electrical aspects to a system-level view of the PUF, specifically to the CRPs (Challenge-Response Pairs) that generate a binary result, where '0' means that $f_{ReferenceRO} < f_{RO}$. This PUF Biasing rate can be estimated by the linear relation $A \cdot \delta T + B$ with $A = 0.49, B = 49.80$ representing technology-dependent parameters.

VI. Conclusion

This paper characterizes the temperature evolution in a Xilinx Spartan-7 FPGA by implementing a "Heating Module" with numerous single-inverter Ring Oscillators (ROs) strategically placed. Findings show a direct proportionality between module size and temperature, along with a non-uniform temperature distribution across the FPGA. The study investigates the impact of heating module-generated temperature on RO frequencies, considering both real-time and permanent thermal effects. Extrapolating the results to a RO-PUF on an ASIC reveals a temperature gradient's influence on PUF responses, with cloning probability directly tied to temperature differences among ROs. The work proposes using this attack for RO-PUF cloning and explores leveraging permanent thermal effects for sustained cloning, potentially evading detection by ASIC temperature detector.

References

[1] François Koeune and François-Xavier Standaert. A tutorial on physical security and side-channel attacks. *International School on Foundations of Security Analysis and Design*, pages 78–108, 2004.

[2] Alessandro Barenghi, Luca Breveglieri, Israel Koren, and David Naccache. Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures. *Proceedings of the IEEE*, 100(11):3056–3076, 2012.

[3] Raghavan Kumar, Harikrishnan Kumarapillai Chandrikakutty, and Sandip Kundu. On improving reliability of delay based physically unclonable functions under temperature variations. In *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*, pages 142–147. IEEE, 2011.

[4] Ranjith Kumar and Volkan Kursun. Voltage optimization for temperature variation insensitive cmos circuits. In *48th Midwest Symposium on Circuits and Systems, 2005.*, pages 476–479. IEEE, 2005.

[5] Aghiles Douadi, Giorgio Di Natale, Paolo Maistri, Elena-Ioana Vatajelu, and Vincent Beroulle. A study of high temperature effects on ring oscillator based physical unclonable functions. In *2023 IEEE 29th International Symposium on On-Line Testing and Robust System Design (IOLTS)*, pages 1–7. IEEE, 2023.

[6] Shengyu Duan and Gaole Sai. Bti aging-based physical cloning attack on sram puf and the countermeasure. *Analog Integrated Circuits and Signal Processing*, pages 1–11, 2023.

[7] Aravinda Koithyar and TK Ramesh. Frequency equation for the submicron cmos ring oscillator using the first order characterization. *Journal of Semiconductors*, 39(5):055001, 2018.

[8] Albert Crespo-Yepes, C Nasarre, N Garsot, Javier Martin-Martinez, R Rodriguez, E Barajas, X Aragones, D Mateo, and Montserrat Nafria. Cmos inverter performance degradation and its correlation with bti, hci and off state mosfets aging. *Solid-State Electronics*, 191:108264, 2022.