electronics

MDPI

Article

Mitigating Thermal Side-Channel Vulnerabilities in FPGA-Based SiP Systems Through Advanced Thermal Management and Security Integration Using Thermal Digital Twin (TDT) Technology

Amrou Zyad Benelhaouare *, Idir Mellal, Maroua Oumlaz and Ahmed Lakhssassi

Department of Engineering and Computer Science, University of Quebec in Outaouais, Gatineau, QC J9A 1L8, Canada; idir.mellal@gmail.com (I.M.); oumm08@uqo.ca (M.O.); ahmed.lakhssassi@uqo.ca (A.L.)

* Correspondence: bena77@uqo.ca

Abstract: Side-channel attacks (SCAs) are powerful techniques used to recover keys from electronic devices by exploiting various physical leakages, such as power, timing, and heat. Although heat is one of the less frequently analyzed channels due to the high noise associated with thermal traces, it poses a significant and growing threat to the security of very large-scale integrated (VLSI) microsystems, particularly system in package (SiP) technologies. Thermal side-channel attacks (TSCAs) exploit temperature variations, risking not only hardware damage from excessive heat dissipation but also enabling the extraction of sensitive data, like cryptographic keys, by observing thermal patterns. This dual threat underscores the need for a synergistic approach to thermal management and security in designing integrated microsystems. In response, this paper presents a novel approach that improves the early detection of abnormal thermal fluctuations in SiP designs, preventing cybercriminals from exploiting such anomalies to extract sensitive information for malicious purposes. Our approach employs a new concept called Thermal Digital Twin (TDT), which integrates two previously separate methods and techniques, resulting in successful outcomes. It combines the gradient direction sensor scan (GDSSCAN) to capture thermal data from the physical field programmable gate array (FPGA), which guarantees rapid thermal scan with a measurement period that could be close to 10 µs, a resolution of 0.5 °C, and a temperature range from −40 °C to 140 °C; once the data are transmitted in real time to a Digital Twin created in COMSOL Multiphysics® 6.0 for simulation using the Finite Element Method (FEM), the real time required by the CPU to perform all the necessary calculations can extend to several seconds or minutes. This integration allows for a detailed analysis of thermal transfer within the SiP model of our FPGA. Implementation and simulations demonstrate that the Thermal Digital Twin (TDT) approach could reduce the risks associated with TSCA by a significant percentage, thereby enhancing the security of FPGA systems against thermal threats.

Keywords: thermal side-channel attacks (TSCA); VLSI; system in package (SiP); thermal management and security; Thermal Digital Twin (TDT); COMSOL Multiphysics®; Finite Element Method (FEM); FPGA; gradient direction sensor scan (GDSSCAN)

check for updates

Citation: Benelhaouare, A.Z.; Mellal, I.; Oumlaz, M.; Lakhssassi, A. Mitigating Thermal Side-Channel Vulnerabilities in FPGA-Based SiP Systems Through Advanced Thermal Management and Security Integration Using Thermal Digital Twin (TDT) Technology. *Electronics* **2024**, *13*, 4176. https://doi.org/10.3390/electronics13214176

Academic Editors: Andrea Guerrieri and Mohamed El-Hadedy Aly

Received: 2 September 2024
Revised: 18 October 2024
Accepted: 21 October 2024
Published: 24 October 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The temperature side-channel (TSC) often gets a nod in the literature [1–8], but most papers simply acknowledge its existence and possible exploitation without really focusing on its security implications. At the early stages of TSCA research, J. Brouchier et al. [3,4] were the first to spotlight the temperature side-channel in 2009. They demonstrated how a cooling fan could unintentionally reveal data by tracking the heat emitted from a processor. In their experiment, they managed to extract bits from a secret password or an RSA key, assuming a low-frequency leakage rate of one bit every three minutes. They also

emphasized that IP cores within FPGAs could expose information to other IP cores through the temperature side-channel.

A few other papers have explored active temperature attacks, where the ambient temperature of a device is intentionally altered (either cooled or heated). Most of these works highlight the success of low-temperature attacks. For instance, S. Skorobogatov [9] and D. Samyde et al. [10] in 2002 demonstrated that by cooling SRAM devices to −50 °C, they could freeze data and retrieve memory contents even several seconds after power was cut, taking advantage of SRAM cells' data-retention properties. T. Müller et al. [11] built on this idea with a tool called FROST, capable of recovering RAM data from modern Android smartphones, much like cold boot attacks on PCs [12]. On the other hand, J.-J. Quisquater and D. Samyde [13] explored high-temperature attacks, noting memory errors after subjecting devices to extended periods of intense heat.

In a recent paper, ref. [14], the authors present the first comprehensive study of a thermal side-channel attack (TSCA), leveraging Intel processors' digital thermal sensors [15–19]. The paper introduces ThermalBleed, marking the first real-world software-based thermal attack. It shows how temperature changes in processors can be exploited to extract sensitive data, like cryptographic keys. This research uncovers new thermal properties, enabling more precise and advanced attacks, thus expanding the attack surface and potentially compromising secure information. Teodora Vasilas's work [20] delves into the growing need to tackle side-channel vulnerabilities as electronic devices become more sophisticated. They build on the Hot-n-Cold anomaly-detection method, adapting it to more practical computing settings by tracking processor temperatures to spot irregularities in Linux command behavior. A key breakthrough in their approach is the introduction of five different noise types (such as file transfers and web browsing) during the attack-detection process. They tested how effectively Hot-n-Cold could monitor temperature changes across three processor types using the ls and chmod Linux commands.

While current research largely focuses on software-based detection of thermal side-channel attacks, hardware analysis remains underexplored. This research aims to bridge the gap by connecting hardware and software solutions through the use of the Digital Twin concept. By creating a virtual replica of the physical system, we will model and simulate how both hardware architecture specifically system in package (SiP) technology, which is becoming increasingly relevant in cyber-physical systems (CPSs) due to its space efficiency and performance advantages, and software-based detection methods interact. Ultimately, the goal is to develop a comprehensive defense strategy that leverages both virtual and physical insights to minimize thermal side-channel vulnerabilities.

In this paper, the idea of connecting hardware and software solutions using the Digital Twin concept for thermal side-channel analysis aligns well with current trends, especially in the context of system in package (SiP) technology. According to recent reviews, SiP is increasingly being adopted in cyber-physical systems (CPSs) because of its ability to integrate multiple ICs into a compact, high-density package, providing both space efficiency and improved performance [21,22]. In terms of research, most of the focus so far has been on software solutions that analyze thermal side-channels, leaving the hardware aspect underexplored. SiP technology, due to its stacked chip architecture and increasing use in CPS applications, presents unique thermal challenges, such as heat dissipation and temperature fluctuations that can be exploited for attacks [23–25]. However, addressing these issues solely from the software side limits the scope of solutions. By using the Digital Twin concept, our research could simulate how thermal interactions between hardware (like SiP components) and software detection mechanisms work together. This would allow us to study and address vulnerabilities more comprehensively. Specifically, SiP's 3D architecture and its reliance on thermal management make it an excellent candidate for studying side-channel leaks. Moreover, this hybrid approach could offer insights into hardware design optimizations, such as better heat-distribution methods or sensor placements, while simultaneously improving software-based anomaly-detection systems. Thus, our proposal to integrate both hardware and software analysis via a Digital Twin will

address a key gap, allowing for more precise, real-world modeling of thermal side-channel vulnerabilities and defense mechanisms. This approach not only complements existing research but also offers a new perspective on designing secure CPS architectures.

1.1. System in Package (SiP) Design

This system in package (SiP) design as depicted in Figure 1 is a heterogeneous system, characterized by the integration of multiple types of components within a single package. In this SiP [26–29], High Bandwidth Memory (HBM DRAM) dies are stacked and connected through Through-Silicon Vias (TSVs) to ensure high-speed data transfer. These memory dies, along with compute and logic dies, are placed on a silicon interposer, which acts as a bridge facilitating communication between the different components. The silicon interposer is connected to the rest of the package through microbumps (µBumps) and C4 copper bumps, which provide dense, high-performance interconnections. The package substrate supports these connections and houses standard package traces for routing signals, while the entire system is connected to the circuit board via package balls and short wires. This diverse combination of HBM DRAM, processing units, interconnection technologies, and structural elements like the silicon interposer and package substrate exemplify the advantages of a heterogeneous system, including enhanced performance, space efficiency, and optimized power consumption.

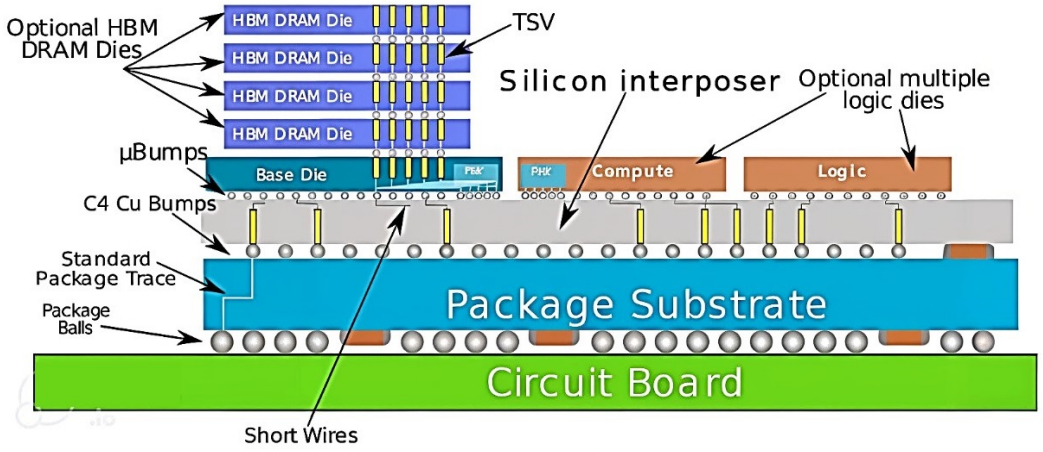


Figure 1. System in package (SiP) design.

The SiP design offers several significant advantages due to its heterogeneous architecture. Firstly, high performance is achieved through reduced latency and efficient data transfer. The integration of High Bandwidth Memory (HBM) with compute and logic dies via Through-Silicon Vias (TSVs) and microbumps ensures faster communication between components, which enhances the overall system performance. Additionally, the presence of multiple compute and logic dies allows for parallel processing, making the system more capable of handling complex tasks efficiently. Secondly, the design provides space efficiency. By vertically stacking memory and other components on the silicon interposer, the SiP minimizes its footprint, which is particularly beneficial for applications requiring compactness, such as mobile devices or small-scale computing systems. Furthermore, the integration of multiple functionalities within a single package reduces the need for additional external components, further conserving space. Thirdly, the SiP is optimized for power efficiency. The close proximity of the components within the package, combined with the use of efficient interconnection technologies like C4 bumps and microbumps, reduces power loss, contributing to lower overall power consumption. The short interconnections, such as TSVs and short wires, also enhance power efficiency compared to traditional multi-chip systems.

In large-scale integrations such as SiP designs, the intricate arrangement of multiple components within a confined space presents significant thermal management challenges. The close proximity of densely packed dies, including memory, logic, and compute units,

inherently accelerates heat transfer across the system. This compact configuration, while beneficial for performance and space efficiency, exacerbates the risk of localized hotspots. As heat rapidly propagates from one component to another, the likelihood of thermal accumulation increases, potentially leading to overheating and compromising the reliability and longevity of the entire system.

1.2. SiP Thermal Challenges

These thermal variations, however, are not always a byproduct of unintentional design complexity. In today's highly interconnected world, with the rise of cyber-physical systems (CPSs) and the Internet of Things (IoT), these fluctuations can also be exploited with malicious intent [30–33]. Cybercriminals may leverage these thermal anomalies to extract sensitive information [34], such as cryptographic keys, by analyzing the heat patterns within these microsystems. The ability to correlate thermal behavior with underlying operations opens the door to reverse engineering technologies, stealing intellectual property, or even replicating security algorithms. Thus, the challenge extends beyond merely managing heat; it necessitates robust thermal security measures to protect against both inadvertent failures and deliberate cyber threats.

In integrated microsystems, particularly those utilizing system in package (SiP) technology, thermal management is critical due to the densely packed components and the complexity of the heat-transfer processes involved. Figure 2 illustrates a simulation conducted using NISA software to analyze a scenario where four heat sources or thermal peaks are randomly distributed within a physical layer [35]. These sources generate localized thermal energy, which diffuses through the material over time.

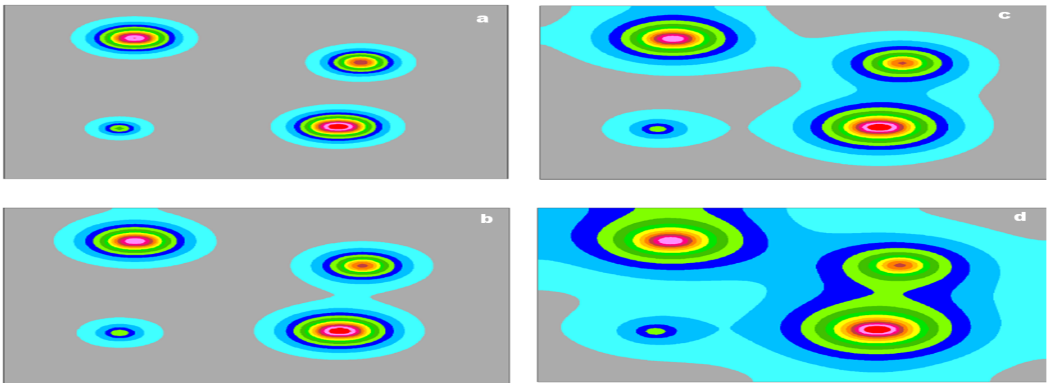


Figure 2. (**a**–**d**) show the thermal evolution over time of four heat sources under the same initial conditions, within a specific layer of the SiP [35].

The phenomenon observed in the image can be understood through the principles of thermal diffusion, governed by the heat equation. The heat equation in three dimensions is given by Equation (1):

$$\frac{\partial T}{\partial t} = \alpha \nabla^2 T + \frac{q'}{\rho c_p} \tag{1}$$

where T is the temperature, q' is the heat flow (W/m^2), α represents the thermal diffusivity (m^2/s), corresponding to the ratio of thermal conductivity to volumetric capacity c_p, ρ is the Material density, and finally $\nabla^2 T$ is the Laplacian operator of T and corresponds in the case of 3D diffusion, to Equation (2)

$$\nabla^2 T = \frac{\delta^2 T}{\delta x} + \frac{\delta^2 T}{\delta y} + \frac{\delta^2 T}{\delta z} \tag{2}$$

Initially, each heat source creates its thermal profile, resulting in distinct isothermal surfaces, as depicted in the individual Figure 2a,b. These surfaces represent regions where

the temperature is constant, forming concentric contours around each heat source. As time progresses, thermal diffusion causes these heat profiles to expand and interact with each other. When multiple heat sources are positioned in close proximity, their thermal fields begin to overlap, as illustrated in Figure 2c,d. The interaction of these thermal fields results in a cumulative effect, where localized areas of high temperature coalesce, potentially forming a large region of intense heat.

In a SiP environment, such thermal interactions pose significant risks. The convergence of multiple heat sources can create hotspots, leading to thermal runaway, a scenario where increasing temperature further accelerates heat generation, potentially resulting in component failure. This is especially concerning in tightly packed 3D architectures, where heat dissipation paths are limited.

The thermal behavior observed here is crucial for understanding and managing the thermal reliability of SiP systems. Without adequate thermal management strategies, these hotspots can degrade the performance and longevity of the entire system, and moreover, they can be exploited by cybercriminals to extract important information through these abnormal thermal variations.

1.3. Foundations and Our Contribution

Thermal attacks targeting large-scale integrated microsystems, such as 3D-SiP, have not been extensively explored in existing literature. The application of these techniques specifically to integrated silicon chips is infrequently discussed in publicly available sources. In the realm of thermal security for silicon chips, the focus has typically been on managing internal heat generation and preventing overheating, rather than implementing defenses against external thermal attacks.

In efforts to improve thermal prediction in very large-scale integration (VLSI) circuits, recent studies [36–39] have revisited the foundational work of Wojciech Wojciak and Andrzej Napieralski from 1997, which introduced the Gradient Direction Sensor (GDS) [40]. This technique utilizes three carefully positioned units of sensors that convert temperature fluctuations into electrical signals, enabling precise measurement of both the direction and magnitude of thermal gradients. Building on this concept, the Surface Peak Thermal Detector Algorithm (STPDA) was developed to enhance the accuracy of heat source identification in electronic components using the GDS.

Further advancements have introduced a hybrid approach that combines the GDS with a Thermal Gradient Tracking (TGT) technique [41]. This new algorithm, known as TGT, employs a recursive method to systematically eliminate areas without significant thermal peaks, focusing on pinpointing regions most likely to exhibit thermal anomalies.

Recent works have also explored the integration of the Finite Element Method (FEM) to model and predict thermal behavior in complex microsystems. Studies and surveys such as those by [42–44] have presented a detail of chip-level thermal simulation techniques developed over the past two decades, aiming to help researchers identify simulators suited to their needs and improve existing techniques.

These foundational advancements, along with ongoing research in real-time thermal monitoring and proactive anomaly detection, form the basis for our contribution. Our work aims to integrate these technologies into a comprehensive Thermal Digital Twin (TDT) framework. This approach not only leverages existing sensor and simulation technologies but also integrates novel methods for early detection of thermal anomalies, particularly in FPGA-based SiP systems, enhancing both performance and security. Additionally, this paper continues the work proposed in our previous conference paper [45], expanding on the initial concept and further validating it through detailed simulations and analysis.

The major contribution of this paper is as follows :

- Innovative TDT Approach :
  - Real-time integration of physical data and numerical simulation (Figure 3):

* GDSSCAN Method: captures real-time thermal data on FPGA-based SiP systems.
* COMSOL (FEM): models and predicts thermal variations in real time using Finite Element Method (FEM).

This methodological progression, combining the precision of physical measurements with the power of numerical simulation, unveils untapped possibilities for diagnosing and addressing thermal and reliability challenges in SiP.

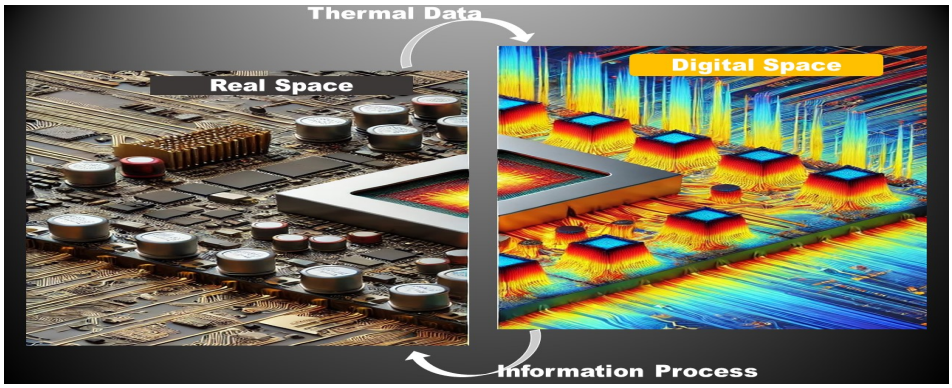


Figure 3. Model of a Thermal Digital Twin (TDT).

The paper is organized as follows: Section 2 details the implementation of the Gradient Direction Sensor (GDS) method for capturing thermal data on physical FPGAs. Specifically, we applied the method to two different FPGA boards, one to test the functionality of the method and the other to validate its effectiveness across different types of boards. Section 3 presents a simulation based on the thermal data collected using the GDS method, enabling a detailed analysis of thermal transfer within the SiP model through the Finite Element Method (FEM). Section 4 discusses a comprehensive comparison between our TDT model and traditional techniques. As part of future work, Section 5 proposes to automate the data-collection and -export processes, enabling efficient communication between the FPGA and COMSOL software to maintain the real-time functionality of our Thermal Digital Twin (TDT). Finally, Section 6 summarizes the key contributions and conclusions of the research.

2. Physical Space: Capturing Thermal Data in FPGA Systems Through Gradient Direction Sensor (GDS) Implementation

FPGAs typically incorporate thermal sensors using ring oscillators, composed of an odd number of inverters. However, this approach has limitations when faced with the dynamic nature of hotspots and the need for comprehensive thermal coverage on large chips. The Gradient Direction Sensor (GDS) technique offers a promising alternative. It could be adapted to perform targeted scanning of areas of interest, thus allowing for a more precise and flexible estimation of heat source temperatures. This method has the advantage of adapting to the spatial evolution of hotspots without requiring a massive deployment of fixed sensors. In the following sections, we will examine in detail the principles and implementation method of the GDS technique in the context of FPGAs.

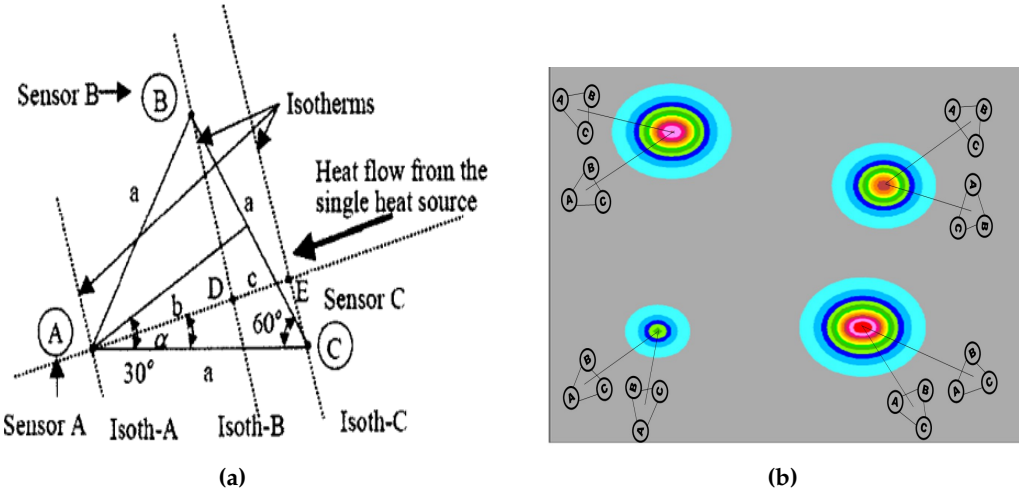
The GDS technique is based on Equation (4), which is designed to calculate the temperature of a heat source based on the frequency variation between two ring oscillators positioned at sensors A and C at a distance 'a' (Figure 4). These ring oscillators are affected by the local temperature: as the temperature increases near a sensor, the oscillation frequency (Equation (3)) decreases, providing a means to estimate the thermal gradient along the line AC. When the heat source is not directly on the AC line, the angles α_1 and α_2 are introduced to correct for this misalignment and provide a more accurate estimate of the thermal gradient (∇T).

$$f_{\mathrm{RO}} = \frac{1}{2 \cdot N \cdot T} \tag{3}$$

where N is the number of delay stages, f_{RO} is the frequency of the ring oscillator, and T is the total delay seen at the output of each stage.

$$\frac{\frac{H}{a}(f_{C_1} - f_{A_1})(\sqrt{3} + \tan\alpha_2)(1 + \tan\alpha_1^2)}{\sqrt{3}(1 - \tan\alpha_1 \tan\alpha_2) - (\tan\alpha_1 + \tan\alpha_2)} + f_{A_1} = f_s \rightarrow T_s \tag{4}$$

The advantage of using ring oscillators is that they provide a measurement of the junction temperature, which reflects the internal thermal state of the chip rather than just the surface or package temperature. The temperature can be measured by calibrating the output of a ring oscillator, which drifts in Hz per °C. This makes the method particularly useful for monitoring hotspots that develop deep within the chip, which might not be detected using surface-mounted sensors alone.



(a) **(b)**

Figure 4. GDS configuration. (**a**) Sensor cell configuration of the GDS technique. (**b**) Placement of the cells consisted of A, B and C sensors in the SiP layer. Color gradients show temperature, with red indicating higher heat at the source.

By utilizing the cell (Figure 4), we can acquire data regarding the temperature distribution and, to some extent, the location of the heat source. Therefore, it is possible to derive Equation (4), which describes the temperature of the heat source.

It is notable that the ISE Xilinx Design software enables implementation and manual positioning of the circuit on the SPARTAN-3E FPGA. Figure 5 depicts the physical arrangement of the three-ring oscillator (RO) sensors, each occupying 0.39 μm^2 on the FPGA.

After the implementation, placement, routing, and deployment of the VHSIC Hardware Description Language (VHDL) code on the FPGA board, the temperature of the heat source was detected to be 69.85 °C, as depicted in Figure 6. This temperature corresponds to a thermal hotspot generated on the board. The ambient temperature of the room where the board is located was 25 °C. We applied additional heat using a hairdryer positioned directly above the board, which generated the heat source, and the GDS method was able to accurately capture this temperature increase.

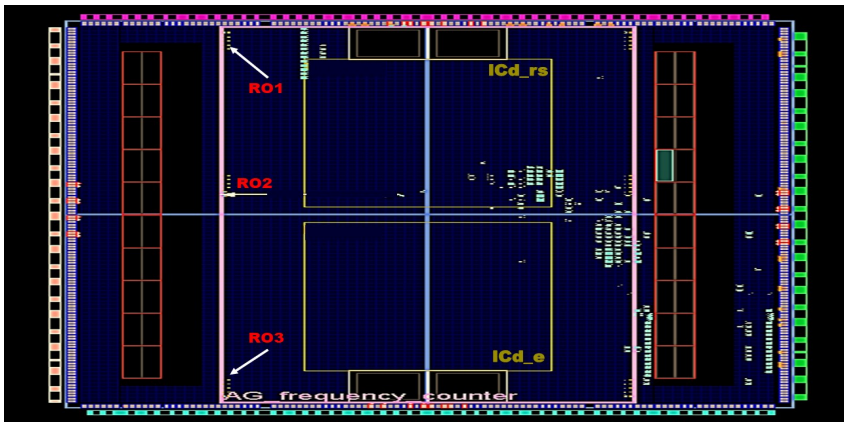


Figure 5. The placement and routing of RO1, RO2, and RO3 on ISE Xilinx Design Tool.

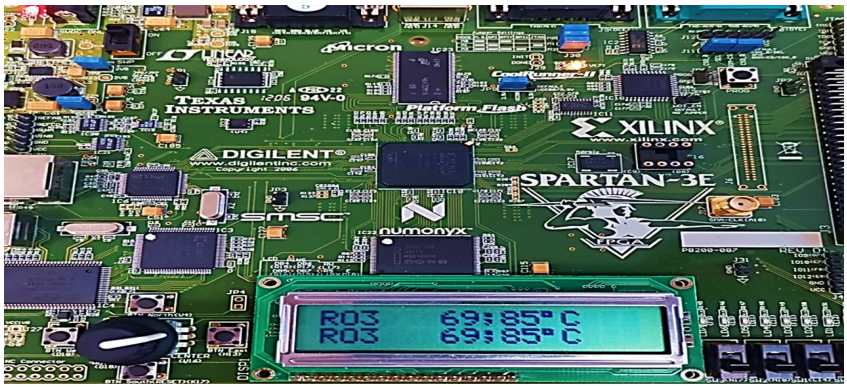


Figure 6. Value of the thermal source detected on Spartan-3E.

To further validate the effectiveness of the Gradient Direction Sensor (GDS) method, we extended its application to an Altera Cyclone V FPGA board. This secondary testing was crucial in ensuring that the GDS method is not only functional on a single type of FPGA but also robust and adaptable across different hardware platforms. The Altera Cyclone V was chosen due to its distinct architecture and thermal characteristics, which differ from the initial Xilinx SPARTAN-3E board used in the preliminary tests. By successfully capturing and analyzing thermal data on Cyclone V as depicted in Figure 7, we confirmed that the GDS method consistently provides accurate measurements of thermal gradients, regardless of the specific FPGA architecture. This cross-validation strengthens the reliability of the GDS technique and demonstrates its potential for broader applicability in diverse FPGA-based systems.

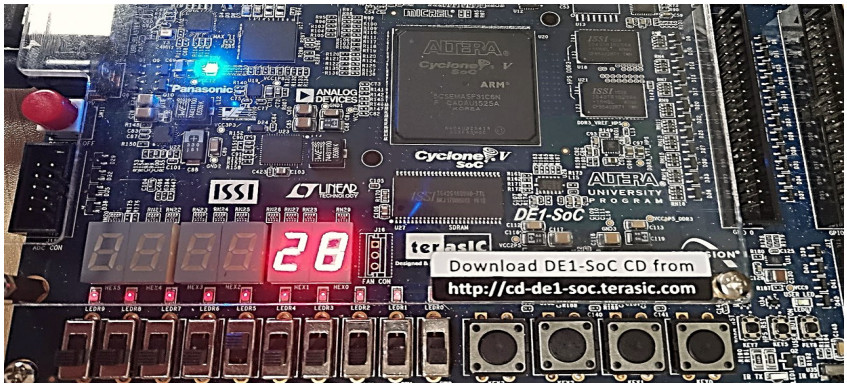


Figure 7. Value of the thermal source detected on Altera Cyclone V.

The selection of the Spartan-3E and Cyclone V FPGA boards was strategically made to validate the effectiveness and adaptability of the GDS method across different architectures and process nodes. The Spartan-3E, with its simpler architecture and larger process node, provides a baseline for thermal behavior with lower integration and fewer thermal hotspots. In contrast, the Cyclone V, utilizing a smaller 28 nm process and more advanced architecture with features like Adaptive Logic Modules (ALMs) and embedded DSP blocks, presents a more complex thermal environment with higher power density and localized heat sources. By successfully applying the GDS method to both boards, we demonstrate its robustness in detecting thermal anomalies across a wide range of FPGA designs, ensuring that the method is effective regardless of architectural or process node variations.

The Gradient Direction Sensor (GDS) method, enhances the detection of thermal side-channel attacks (TSCA) by leveraging accurate thermal peak detection and real-time monitoring. The GDS method integrated with a ring oscillator (RO) measures the frequency changes due to temperature variations. Here are the key measurable performance metrics and frequencies from the studies [35,36] that demonstrate the effectiveness of this method:

- Measured Frequency–Temperature Response: The normalized response of the ring oscillator shows a strong correlation between temperature changes and frequency adjustments, ensuring that even small temperature differences are detectable. This is crucial for early detection of TSCA, where even minor temperature variations can signal data leakage.
- Power Density and Temperature Gradient: With power densities reaching 20 W in critical zones, the GDS method was able to predict thermal peaks at a maximum temperature of 103.3 °C, with a temperature gradient ($\triangle$T) of 11.15 °C across the structure. This highlights the method's effectiveness in handling high power densities while maintaining precise thermal monitoring.

So, the integration of the GDS method in our TDT offers the following:

- Real-time monitoring with the ability to detect thermal fluctuations as they happen, along with proactive responses to prevent TSCA before significant thermal differences arise. However, the traditional thermal management approaches are typically reactive, addressing heat issues only after they have been detected, often through static temperature thresholds or periodic monitoring. This makes it easier for attackers to exploit delays in thermal response.

Despite its advantages, GDS has some limitations:

- Computational Overhead: Continuous real-time monitoring and analysis of thermal gradients can consume significant computational resources, potentially impacting the overall system performance, especially in resource-constrained environments like FPGA-based SiP systems. This overhead can reduce the system's throughput and efficiency.
- Sensor Calibration: The accuracy of GDS heavily depends on the calibration of sensors. Any errors or miscalibrations in sensor placement or thermal data collection can lead to inaccurate gradient detection, undermining the security against TSCA.

Ultimately, the value of the heat source is detected using the GDS method, which has been previously employed in other studies and is reused in this work due to its effectiveness and precision. These thermal data, expressed in Celsius, serve as the foundation and initial conditions in the digital domain for monitoring and analyzing thermal transfer within the SiP.

3. Numerical Space: Thermal Transfer Simulation in SiP Models Using FEM Based on GDS-Collected Data

Several methodologies exist for simulating and modeling heat transfer within a 3D integrated circuit. This study employs the COMSOL Multiphysics® commercial simulator, a widely adopted Finite Element Method (FEM) based on discretization. It encompasses

various modules, notably a dedicated heat-transfer module tailored for thermal simulation. With its highly efficient thermal capabilities and graphical circuit-modeling features, this tool simplifies circuit modeling. Our selection aligns with current industry trends, given its widespread use and reliability in analyzing complex concepts.

We conducted simulations on a specific configuration of 3D-SiP. This assembly consists of four vertically stacked silicon chips interconnected by micro-bumps and modeled in 3D using the finite element software COMSOL Multiphysics®, as illustrated in Figure 8.

The properties and materials used in this thermal finite element modeling of our 3D-SiP with COMSOL Multiphysics® are summarized in Table 1 [45].

Table 1 provides an overview of the characteristics and materials employed in the Finite Element Method (FEM) modeling presented in this study.

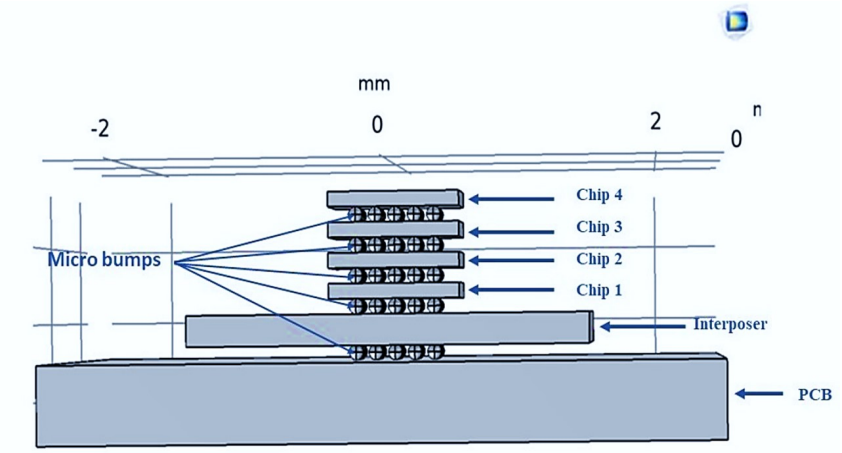


Figure 8. Modeling the SiP with 4 vertically stacked silicon chips.

Table 1. Physical properties of the SiP.

Properties	SiP (FR4)	4 Chips and Interposer Layer (Silicon)	Micro-Bumps (Copper)
Heat capacity at constant pressure (J/Kg·K)	1369	700	385
Density (Kg/m^3)	1900	2329	8960
Thermal conductivity (W/m·K)	0.3	130	400

When heat is generated on the surface of a die, it can follow different thermal paths (see Figure 9). The heat transfer might occur vertically through layers within the same stack where it was generated or horizontally to adjacent stacks. The heat generated in one die can affect all other dies in the system, with the junction temperature being calculated as the sum of contributions from self-heating, ambient temperature, and the coupling effects from heat generation in other dies. Once heat is generated, it propagates through the layers (see Figure 10), raising their temperature. Each layer responds differently to heat, with the temperature increasing depending on its thermal properties, the amount of heat, and its distance from the heat source.

Figure 9 vividly illustrates the dissipation process, depicting the definition of boundary conditions for the SiP. We utilized the value of the detected thermal peak from the physical space as elaborated in Section 2 as a basis for analyzing heat dissipation within the SiP.

The direction of heat dissipation and transfer is indicated by the blue arrows. Three distinct pathways are discernible: one ascending towards the encapsulation case or the

surrounding ambient air, a second directed upwards towards the SiP, and a third leading towards the SiP. Upon observing the simulation results, it becomes evident that the highest temperature, reaching 69.95 °C, is situated on chip 1, aligning with our predefined boundary conditions. In contrast, the lowest temperature, approximately 20.81 °C, is localized at the base of the SiP, which serves as the foundational component of the system.

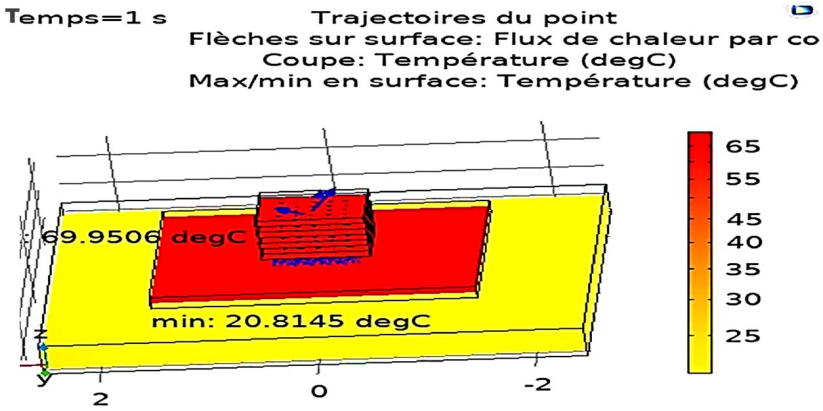


Figure 9. SiP Thermal Digital Twin simulation.

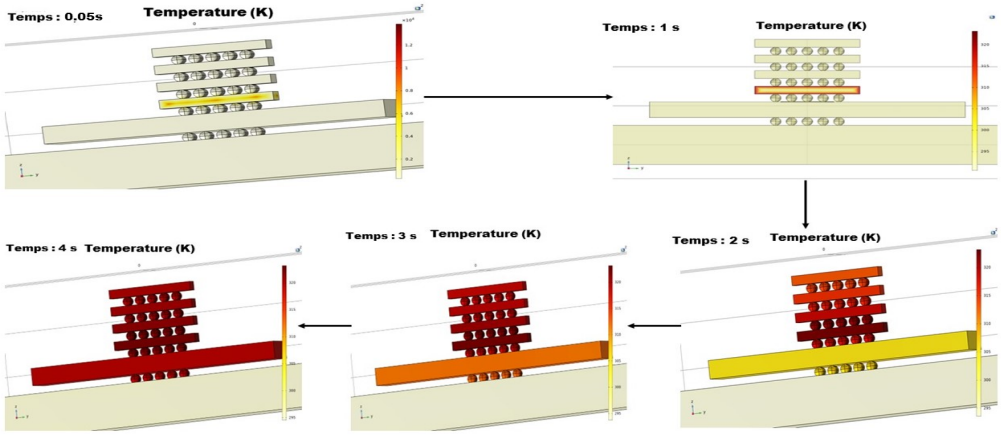


Figure 10. Transient temperature distribution across dies and layers obtained through FEM simulation.

4. Discussion

While Digital Twin (DT) technologies have been successfully studied and widely adopted across various sectors such as agriculture, education, healthcare, manufacturing and industry, automotive, security, smart cities, and weather forecasting, their use in the thermal management of system in package (SiP) remains unexplored in the literature. Applying DT to optimize thermal prediction for SiPs represents a novel contribution. This new approach is aimed at refining thermal forecasts for SiPs.

Our proposal for a Thermal Digital Twin (TDT) as depicted in Figure 11, leveraging both the technological advancements of the Gradient Direction Sensor (GDS) introduced by Wojciech Wojciak and Andrzej Napieralski in 1997 [40] and the Finite Element Method (FEM) in COMSOL Multiphysics®, constitutes a significant advancement in predicting the thermal dynamics of electronic microsystems. Unlike previous works that focused either on the independent application of the GDS for thermal monitoring of semiconductor devices [35,36] or on the exclusive use of FEM to model the thermal performance of 3D-SiP assemblies, our method integrates these two approaches into an advanced simulation model.

The integration of the GDS method into our TDT provides several benefits, including real-time monitoring that detects thermal fluctuations as they occur and enables proactive

responses to prevent TSCA before significant thermal variations develop. In contrast, traditional thermal management approaches tend to be reactive, addressing heat issues only after they are detected, often relying on static temperature thresholds or periodic monitoring, which can leave room for attackers to exploit delays in the system's thermal response. However, the GDS method has some limitations:

- Computational Overhead: Continuous real-time monitoring and analysis of thermal gradients require considerable computational resources, which can impact overall system performance, particularly in resource-limited environments like FPGA-based SiP systems, potentially reducing throughput and efficiency.
- Sensor Calibration: The accuracy of GDS relies heavily on precise sensor calibration. Any miscalibration or errors in sensor placement and data collection can result in inaccurate gradient detection, weakening the system's defense against TSCA.

The FEM in multi-layered systems such SiP offers temperature-prediction accuracy within 1% to 4% as highlighted by [44] and is crucial for preventing thermal-induced failures and enhancing security against TSCA in FPGA systems. Compared to other numerical methods, FEM outperforms the Finite Difference Method (FDM), which, while faster and easier to implement, lacks accuracy in complex, multi-material systems like SiP. Green's Function-based methods provide significantly faster computations by simplifying the heat equation, but they sacrifice accuracy, especially in transient thermal scenarios, making FEM more suitable for detailed thermal analysis.

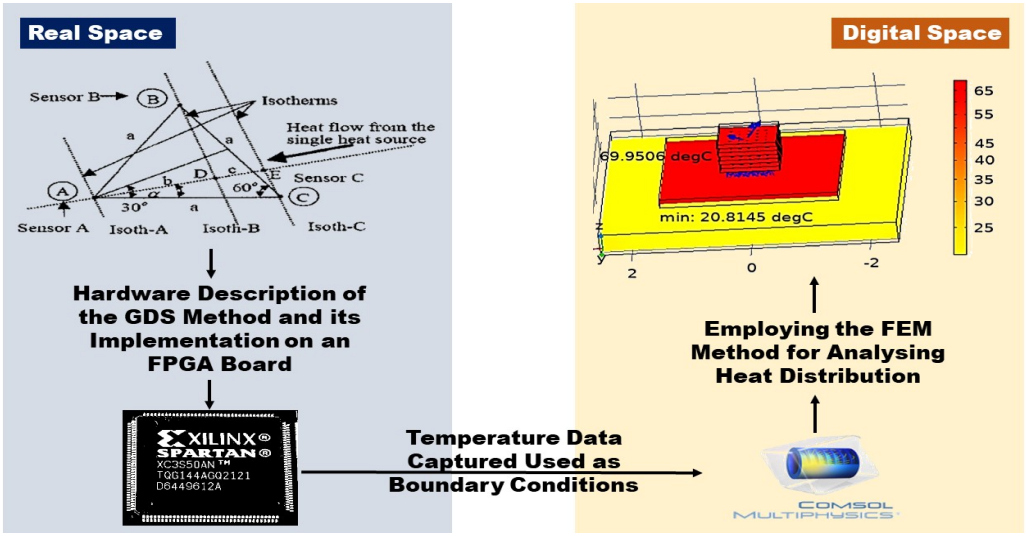


Figure 11. Scheme of a TDT.

To sum up, The GDS, with its innovative principle of directional gradient detection using three strategically placed sensors offer a precise approach for identifying point heat sources on semiconductor devices. However, this method, while effective for local and accurate measurements, is limited in its ability to provide an overview of the complex thermal behavior of integrated systems on a large scale. On the other hand, the use of FEM in COMSOL Multiphysics® for heat-transfer analysis, as demonstrated by Amrou Ziad Benelhaouare and his team [45], allows for detailed modeling and simulation of the thermal performance of 3D-SiP configurations. This approach excels in predicting thermal viability and formulating optimized thermal management strategies, but can be complex in terms of computation for real-time applications.

5. Future Work: Automating the Transfer of Thermal Data in TDT

Building upon the foundation of real-time thermal simulation in FPGAs, our proposed future work aims to revolutionize the concept of Thermal Digital Twins (TDTs) by creating a seamless, intelligent bridge between the physical FPGA and its digital counterpart, while

also enhancing security against thermal side-channel attacks (TSCA). This advanced TDT system will automate the transfer of thermal data from integrated sensors to the COMSOL simulation environment, enhancing the fidelity and utility of the digital model. Key aspects of this system include the following:

- Secure data transmission from the FPGA to an intermediate processing system (microcontroller or computer) via encrypted standard protocols such as Inter-Integrated Circuit (I2C), Serial Peripheral Interface (SPI), or Controller Area Network (CAN) (Figure 12). For wireless transmission, Wi-Fi or Bluetooth modules with enhanced security features can be integrated into the FPGA.
- A dedicated interface program on the intermediate system that receives the data, authenticates them, and formats them for direct integration into the COMSOL model while monitoring for anomalous thermal patterns that could indicate a TSCA attempt.
- Real-time updating of the Digital Twin in COMSOL, which instantly interprets the received data and updates the thermal model, incorporating algorithms to detect and mitigate potential thermal side-channel leaks.
- Continuous simulation and analysis of thermal behavior based on the received data, enabling real-time analysis of the FPGA's thermal profile and identification of suspicious thermal variations that might suggest a TSCA in progress.

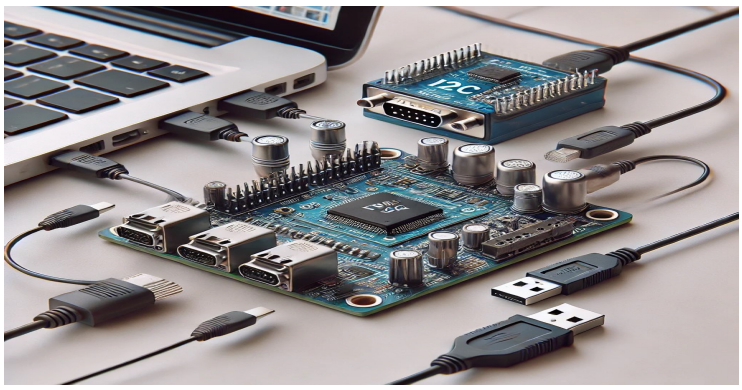


Figure 12. I2C standard protocol.

By implementing machine learning algorithms directly on the FPGA for data preprocessing and TSCA detection, developing edge computing architectures for initial analysis and security screening, and exploring adaptive sampling techniques, we aim to optimize data flow, reduce latency, and enhance security against thermal-based attacks. The integration of multi-sensor fusion, advanced wireless protocols with robust encryption, and AI-driven predictive modeling will enable a more comprehensive, forward-looking, and secure thermal analysis. This holistic approach to TDT development will significantly enhance our ability to predict, manage, and optimize thermal behavior in real-time, while also fortifying the system against thermal side-channel attacks, leading to more efficient, reliable, thermally aware, and secure FPGA designs. Ultimately, this research will pave the way for next-generation thermal management strategies in complex integrated systems, addressing critical challenges in power efficiency, reliability, performance optimization, and security against emerging thermal-based threats.

6. Conclusions

The integration of the Thermal Digital Twin (TDT) model with system in package (SiP) thermal management systems marks a significant advancement in addressing the dual challenges of excessive heat dissipation and thermal side-channel attacks (TSCA) in FPGA-based systems. By combining the gradient direction sensor scan (GDSSCAN) with Finite Element Method (FEM) simulations in COMSOL Multiphysics®, this approach allows for more precise real-time detection of thermal anomalies, enabling proactive measures to prevent potential security vulnerabilities. The research demonstrates that through the novel

use of TDT, it is possible to enhance both the performance and security of FPGA-based SiP systems. By effectively detecting abnormal thermal fluctuations early, this method offers a robust solution for mitigating risks associated with TSCA, thereby contributing to the overall security and reliability of modern VLSI microsystems. The combination of localized thermal detection with system-level simulation bridges a gap in the current literature, providing a comprehensive approach to thermal management and security integration.

Future work will focus on automating the real-time data transfer from FPGA sensors to the COMSOL simulation environment, further optimizing the system for both performance and security. This continued development of the TDT concept will pave the way for more secure and thermally efficient designs in the context of cyber-physical systems (CPSs).

Author Contributions: A.Z.B. developed the first version of the proposal, conceived the idea, and is the innovator behind the concept. He also produced all the results shown in the article, including those under the images. I.M. collaborated with me to validate the simulations and the technical implementation of the techniques discussed in the article. M.O. assisted with the English revision and reformulation to strengthen the language of the paper. A.L., as the senior author and a thermal modeling specialist, supervised all stages of the work, from conceptualization to writing and revision of the paper. All authors have read and agreed to the published version of the manuscript

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: All authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflicts of interest.

References

1. Bar-El, H.; Choukri, H.; Naccache, D.; Tunstall, M.; Whelan, C. The sorcerer's apprentice guide to fault attacks. *Proc. IEEE* **2006**, *94*, 370–382. [CrossRef]
2. Barenghi, A.; Breveglieri, L.; Koren, I.; Naccache, D. Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures. *Proc. IEEE* **2012** *100*, 3056–3076. [CrossRef]
3. Brouchier, J.; Dabbous, N.; Kean, T.; Marsh, C.; Naccache, D. Thermocommunication. *Cryptology ePrint Archive* 2009. Available online: https://eprint.iacr.org/2009/002 (accessed on 1 September 2024).
4. Brouchier, J.; Kean, T.; Marsh, C.; Naccache, D. Temperature attacks. *Temp. Attacks. IEEE Secur. Priv.* **2009**, *7*, 79–82. [CrossRef]
5. Hutter, M.; Schmidt, J.M.; Plos, T. RFID and its vulnerability to faults. In *Cryptographic Hardware and Embedded Systems–CHES 2008: 10th International Workshop, Washington, DC, USA, Proceedings 10*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 363–379.
6. Karaklajić, D.; Schmidt, J.M.; Verbauwhede, I. Hardware designer's guide to fault attacks. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2013**, *21*, 2295–2306. [CrossRef]
7. Otto, M. Fault Attacks and Countermeasures. Doctoral Dissertation, University of Paderborn, Paderborn, Germany, 2005.
8. Schmidt, J.M.; Hutter, M. Optical and em Fault-attacks on Crt-Based Rsa: Concrete Results. In Proceedings of the 15th Austrian Workshop on Microelectronics, Graz, Austria, 11 October 2007; p. 9.
9. Skorobogatov, S. *Low Temperature Data Remanence in Static RAM (No. UCAM-CL-TR-536)*; University of Cambridge, Computer Laboratory: Cambridge, UK, 2002.
10. Samyde, D.; Skorobogatov, S.; Anderson, R.; Quisquater, J.J. On a new way to read data from memory. In Proceedings of the First International IEEE Security in Storage Workshop, Greenbelt, MD, USA, 11 December 2002; pp. 65–69.
11. Müller, T.; Spreitzenbarth, M. FROST: Forensic recovery of scrambled telephones. In *Applied Cryptography and Network Security: 11th International Conference, ACNS Canada. Proceedings 11*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 373–388.
12. Halderman, J.A.; Schoen, S.D.; Heninger, N.; Clarkson, W.; Paul, W.; Calandrino, J.A.; Feldman, A.J.; Appelbaum, J.; Felten, E.W. Lest we remember: Cold-boot attacks on encryption keys. *Commun. ACM* **2009**, *52*, 91–98. [CrossRef]
13. Quisquater, J.J.; Samyde, D. Eddy current for magnetic analysis with active sensor. In Proceedings of the eSMART, Nice, France, 16 December 2002; pp. 185–194.
14. Kim, T.; Shin, Y. ThermalBleed: A Practical Thermal Side-Channel Attack. *IEEE Access* **2022**, *10*, 25718–25731. [CrossRef]
15. Famille de Processeurs Intel Xeon E5-2400, Mountain View, CA, États-Unis: Intel. Available online: https://ark.intel.com/content/www/fr/fr/ark/products/series/59138/intel-xeon-processor-e5-family.html (accessed on 16 October 2024).
16. Famille de Processeurs Intel Xeon Scalable Family, Mountain View, CA, États-Unis: Intel. Available online: https://www.intel.fr/content/www/fr/fr/products/details/processors/xeon/scalable.html (accessed on 16 October 2024).
17. Intel® Core™ Processor Family. Available online: https://www.intel.com/content/www/us/en/products/details/processors/core.html (accessed on 16 October 2024).

18. CPU Cooler: Liquid Cooling vs. Air Cooling. Available online: https://www.intel.com/content/www/us/en/gaming/resources/cpu-cooler-liquid-cooling-vs-air-cooling.html (accessed on 16 October 2024).
19. Information about Temperature for Intel® Processors. Available online: https://www.intel.com/content/www/us/en/support/articles/000005597/processors.html (accessed on 16 October 2024).
20. Vasilas, T.; Bacila, C.; Brad, R. Beat the Heat: Syscall Attack Detection via Thermal Side-Channel. *Future Internet* **2024**, *16*, 301. [CrossRef]
21. Wang, H.; Ma, J.; Yang, Y.; Gong, M.; Wang, Q. A review of system-in-package technologies: Application and reliability of advanced packaging. *Micromachines* **2023**, *14*, 1149. [CrossRef]
22. Criado, J.; Asensio, J.A.; Padilla, N.; Iribarne, L. Integrating cyber-physical systems in a component-based approach for smart homes. *Sensors* **2018**, *18*, 2156. [CrossRef]
23. Kim, N.Y.; Rathore, S.; Ryu, J.H.; Park, J.H.; Park, J.H. A survey on cyber physical system security for IoT: Issues, challenges, threats, solutions. *J. Inf. Process. Syst.* **2018**, *14*, 1361–1384.
24. Wang, Z.; Xie, W.; Wang, B.; Tao, J.; Wang, E. A survey on recent advanced research of CPS security. *Appl. Sci.* **2021**, *11*, 3751. [CrossRef]
25. Agrawal, N.; Kumar, R. Security perspective analysis of industrial cyber physical systems (I-CPS): A decade-wide survey. *ISA Trans.* **2022**, *130*, 10–24. [CrossRef] [PubMed]
26. Lau, J.H. Recent advances and trends in multiple system and heterogeneous integration with TSV interposers. *IEEE Trans. Compon. Packag. Manuf. Technol.* **2023**, *13*, 3–25. [CrossRef]
27. Liu, M.; Zhou, Y.; Dai, J.; Qiao, Q.; Wang, J.; Chen, K. A novel 3D packaging technology for high-reliability applications. In Proceedings of the 24th International Conference on Electronic Packaging Technology (ICEPT), Shihezi, China, 8–11 August 2023; pp. 1–4.
28. Loh, G.H. 3D-Stacked Memory Architectures for Multi-core Processors. *ACM Sigarch Comput. Archit. News* **2008**, *36*, 453–464. [CrossRef]
29. Sami, M.S.U.I.; Zhang, T.; Shuvo, A.M.; Haque, M.S.U.; Calzada, P.E.; Azar, K.Z.; Kamali, H.M.; Rahman, F.; Farahmandi, F.; Tehranipoor, M. Advancing Trustworthiness in System-in-Package: A Novel Root-of-Trust Hardware Security Module for Heterogeneous Integration. *IEEE Access* **2024**. [CrossRef]
30. Lesch, V.; Züfle, M.; Bauer, A.; Iffländer, L.; Krupitzer, C.; Kounev, S. A literature review of IoT and CPS—What they are, and what they are not. *J. Syst. Softw.* **2023**, *200*, 111631. [CrossRef]
31. Peng, H.; Liu, C.; Zhao, D.; Ye, H.; Fang, Z.; Wang, W. Security analysis of CPS systems under different swapping strategies in IoT environments. *IEEE Access* **2020**, *8*, 63567–63576. [CrossRef]
32. Dafflon, B.; Moalla, N.; Ouzrout, Y. The challenges, approaches, and used techniques of CPS for manufacturing in Industry 4.0: A literature review. *Int. J. Adv. Manuf. Technol.* **2021**, *113*, 2395–2412. [CrossRef]
33. Lu, Y. Cyber Physical System (CPS)-Based Industry 4.0: A Survey. *J. Ind. Integr. Manag.* **2017**, *2*, 1750014. [CrossRef]
34. Kok, C.L. A Novel Study on a 300 °C, High Performance LDO Regulator Using Silicon-On-Insulator Process for Extreme Drill Bit Application. In Proceedings of the IEEE 19th International SoC Design Conference (ISOCC), Gangneung-si, Republic of Korea, 19–22 October 2022; pp. 286–289.
35. Bougataya, M.; Lakhsasi, A.; Massicotte, D. VLSI thermo-mechanical stress analysis by gradient direction sensor method. In Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering, Saskatoon, SK, Canada, 1–4 May 2005; pp. 710–713.
36. Lakhssassi, A.; Bougataya, M.; Boustany, C.; Massicotte, D. Thermal stress monitoring using gradient direction sensors. In Proceedings of the 6th International IEEE Northeast Workshop on Circuits and Systems and TAISA Conference, Montreal, QC, Canada, 22–25 June 2008.
37. Szermer, M.; Janicki, M.; Kulesza, Z.; Napieralski, A. Practical realization of PTAT sensor for ASIC overheat protection. In Proceedings of the IEEE 15th International Workshop on Thermal Investigations of ICs and Systems, Leuven, Belgium, 7–9 October 2009; pp. 80–83.
38. Szermer, M.; Janicki, M.; Pietrzak, P.; Kulesza, Z.; Napieralski, A. PTAT sensor for chip overheat protection. In Proceedings of the 26th Annual IEEE Semiconductor Thermal Measurement and Management Symposium (SEMI-THERM), Santa Clara, CA, USA, 21–25 February 2010; pp. 176–179.
39. Lahbacha, K. Electrothermal Analysis of Memristors and Thermistors. Doctoral Dissertation, Università Degli Studi di Cassino e Del Lazio Meridionale, Cassino, Italy, 2022. Available online: https://iris.unicas.it/bitstream/11580/91719/1/TESI_DOTTORATO_UNICAS_34_LAHBACHA_KHITEM.pdf (accessed on 1 September 2024).
40. Wójciak, W.; Napieralski, A. Thermal monitoring of a single heat source in semiconductor devices—The first approach. *Microelectron. J.* **1997**, *28*, 313–316. [CrossRef]
41. Touati, D.E.; Oukaira, A.; Hassan, A.; Ali, M.; Lakhssassi, A.; Savaria, Y. Accurate On-Chip Thermal Peak Detection Based on Heuristic Algorithms and Embedded Temperature Sensors. *Electronics* **2023** *12*, 2978. [CrossRef]
42. Lu, T.; Zhang, F.; Jin, J.M. Multiphysics simulation of 3-D ICs with integrated microchannel cooling. *IEEE Trans. Compon. Packag. Manuf. Technol.* **2016**, *6*, 1620–1629. [CrossRef]
43. Tsai, M.; Wang, Y.; Liu, C.-M. Thermally-Induced Deformations and Warpages of Flip-Chip and 2.5D IC Packages Measured by Strain Gauges. *Materials* **2021**, *14*, 3723. [CrossRef] [PubMed]

44. Sultan, H.; Chauhan, A.; Sarangi, S.R. A survey of chip-level thermal simulators. *ACM Comput. Surv. (CSUR)* **2024**, *52*, 1–35. [CrossRef]
45. Benelhaouare, A.Z.; Oukaira, A.; Oumlaz, M.; Lakhssassi, A. Enhancing Thermal Security of 3D-SiP Systems through Thermal Digital Twin (TDT). In Proceedings of the 2024 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Kingston, ON, Canada, 6–9 August 2024; pp. 20–24.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.