

ChipletQuake: On-die Digital Impedance Sensing for Chiplet and Interposer Verification

Saleh Khalaj Monfared
Worcester Polytechnic Institute
Worcester, MA
skmonfared@wpi.edu

Maryam Saadat Safa
Worcester Polytechnic Institute
Worcester, MA
msafa@wpi.edu

Shahin Tajik
Worcester Polytechnic Institute
Worcester, MA
stajik@wpi.edu

Abstract—The increasing complexity and cost of manufacturing monolithic chips have driven the semiconductor industry toward chiplet-based designs, where smaller and modular chiplets are integrated onto a single interposer. While chiplet architectures offer significant advantages, such as improved yields, design flexibility, and cost efficiency, they introduce new security challenges in the horizontal hardware manufacturing supply chain. These challenges include risks of hardware Trojans, cross-die side-channel and fault injection attacks, probing of chiplet interfaces, and intellectual property theft. To address these concerns, this paper presents *ChipletQuake*, a novel on-chiplet framework for verifying the physical security and integrity of adjacent chiplets during the post-silicon stage. By sensing the impedance of the power delivery network (PDN) of the system, *ChipletQuake* detects tamper events in the interposer and neighboring chiplets without requiring any direct signal interface or additional hardware components. Fully compatible with the digital resources of FPGA-based chiplets, this framework demonstrates the ability to identify the insertion of passive and subtle malicious circuits, providing an effective solution to enhance the security of chiplet-based systems. To validate our claims, we showcase how our framework detects Hardware Trojan and interposer tampering.

Index Terms—Hardware Security, Hardware Trojans, Power Delivery Network, Tamper Detection, Chiplet Security

I. INTRODUCTION

The increasing complexity of monolithic chips has led to skyrocketing costs and significant technical challenges over the last decade. As semiconductor manufacturers push towards smaller nodes, the sophistication of scaling down components while maintaining performance, power efficiency, and cost becomes more difficult. On the other hand, manufacturing large-scale System-On-Chips (SoC) brings significant challenges regarding post-silicon testing procedures. In response, the industry has shifted towards multi-chip module (MCM) designs, where multiple smaller chiplets are integrated onto a single interposer. Such heterogeneous packaging approaches offer several advantages, such as allowing the combination of different process technologies, improving yields by using smaller, modular dies, and enhancing scalability.

Contrary to monolithic ICs, creating systems from separately produced components creates security issues, e.g., the possibility of die-swapping, susceptibility to interposer probing, or tampering. In a zero-trust security model, a chiplet should be able to verify other chiplets. Verification schemes such as delay-based PUFs between chiplets have

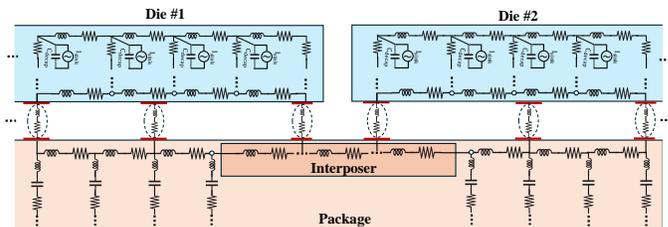


Fig. 1: A simple circuit model of a PDN and interposer inspired by [4].

been developed, where the signal propagation delays through the interposers are considered as fingerprints [1]. However, there might be no direct signal connection between the verifier and prover chiplets to realize such PUFs. Moreover, there could be sophisticated probing or tampering attacks on chiplets interfaces [2], which enable direct eavesdropping from the interposer wires.

In MCMs, multiple chiplets and interposers are interconnected through a shared power distribution network (PDN). Fig. 1 shows a simple model of a PDN and interposer. The PDN distributes power from a central source to each chiplet. There have been a few attempts in the literature [3] to include self-contained sensors on one of the chiplets to detect anomalies in adjacent chiplets. On digital ICs and field-programmable gate arrays (FPGAs), these sensors take the form of delay-based circuits such as on-chip ring-oscillators and time-to-digital converters. If all goes well, any anomalies in running applications will then affect the sensitive timing behavior of these sensors. However, such passive sensing methods have led to low-precision measurements and noisy behavior. Therefore, advanced machine learning methods are needed to obtain acceptable classification accuracy. Moreover, all these solutions only demonstrate the detection of specific anomaly behavior in running software and are not applicable to physical tamper events, such as dormant hardware Trojans. Hence, it remains open if we can have a sensor on a trusted chiplet that can physically verify its environment beyond itself, from the interposer to neighboring chiplets, in a unified manner.

Contribution. In this work, we show that circuit-level

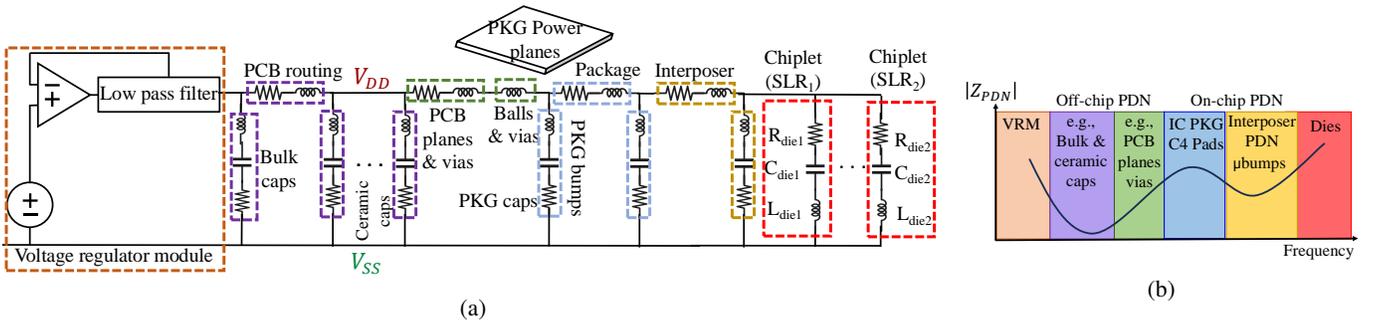


Fig. 2: (a) Equivalent RLC circuit model of the power distribution network of the PCB and chip. (b) Contribution of different parts of the PDN to the impedance over frequency [5].

elements (in terms of their hardware placements and routing) can be potentially fingerprinted in a PDN-shared heterogeneous system that is organized with multiple chiplets in a single package. Our method relies on the fact that physical modifications (regardless of their physical size, activation, or action characteristics) alter the impedance of the shared PDN. Therefore, characterizing the impedance can lead to the detection of the tamper events. Although such PDN-based signatures are studied for chiplet fingerprinting as a possible attack vector in multi-tenant cloud FPGAs [6], we aim to show that chiplet and interposer monitoring is possible for security verification. For this purpose, we present a systematic frequency-sweeping mechanism that can identify the integrity of the internal circuitry of the chiplets and the corresponding interposer interconnection circuits. In summary, the key contributions of this manuscript are as follows:

- This article is the first work to introduce a fully-digital and spectral-assisted method to accurately ensure the hardware integrity of chiplets.
- We design a framework, namely *ChipletQuake*, which provides efficient and effective hardware verification of adjacent chiplets and host interposer.
- We implement *ChipletQuake* on a high-end chiplet-based FPGA system and perform extensive experiments against real-world hardware Trojans, and showcase the applicability of our framework.

II. TECHNICAL BACKGROUND

A. Power Delivery Network (PDN)

The Power Delivery Network (PDN) is critical in providing a stable and low-noise voltage supply to the electronic components on a PCB, spanning from the voltage regulator module (VRM) to the power rails on the chip. The PDN is made up of both off-chip and on-chip elements, such as bulk capacitors, PCB routing, ceramic capacitors, PCB planes, vias, package bumps, on-chip power planes, and transistor capacitance. In the case of multi-die systems, interposer, and its corresponding μ bumps, inter-die interconnections are also part of the PDN. Each of these components contributes to the PDN's impedance across different frequency regimes.

At low frequencies, the impedance of the PDN is primarily governed by the voltage regulator and off-chip components. As the frequency increases, the impedance behavior changes significantly, with the on-chip components contributing more to the PDN impedance at higher frequencies. This shift is largely due to parasitic inductance inherent in each capacitor, which affects their behavior at different frequencies. At higher frequencies, capacitors exhibit a resonance phenomenon caused by the parasitic inductance in their metals. Beyond this resonance frequency, the capacitors behave like open circuits, drastically reducing their impact on the PDN's impedance. Smaller capacitors, with lower parasitic inductance, resonate at higher frequencies, meaning their influence on the PDN impedance diminishes as the frequency increases. Consequently, at very high frequencies, the impedance is dominated by interposer and on-chip structures, which are characterized by smaller dimensions.

The on-chip PDN behavior is modeled using an equivalent RC circuit, where the on-chip capacitance is represented by multiple narrow-band parallel RC circuits connected to the VDD and VSS power rails, see Fig. 2. These circuits allow for an accurate representation of the PDN impedance over a wide frequency range. The impedance characteristics of the PDN in the frequency domain provide valuable insight into the behavior of the system and can even be used to detect tampering events at the PCB level. Tampering with components inside the integrated circuit (IC), such as altering logic gates, placement, or routing, can change the on-chip capacitance, which in turn affects the PDN's impedance. This impact depends on the size, location, and nature of the tampering, demonstrating the sensitivity of the PDN to modifications within the chip [5].

B. Interposer Power Distribution Network

Today's PDN design for multi-chip modules is meticulously designed to manage the high power demands of large-scale compute circuits while maintaining signal integrity and effective thermal management. In this particular work, we focus on Xilinx/AMD's Stacked Silicon Interconnect (SSI) technology, which provides chiplet-based interconnections in multi-chip FPGAs. At the core of this architecture is the silicon interposer, a passive layer that facilitates routing for con-

figuration, global clocking, and interconnect signals between the programmable logic units known as Xilinx’s Super Logic Regions (SLRs). Each SLR in the SSI-enabled device operates with independent power delivery, with power and ground connections routed through the interposer. These connections are facilitated by Through-Silicon Vias (TSVs), which create low-resistance paths between the active layers of the FPGA and the package substrate. This segmentation minimizes cross-talk between regions, enhancing both power delivery efficiency and overall signal integrity.

The interposer enables the use of separate power planes for core logic, I/O, transceivers, and memory interfaces, reducing electrical noise and ensuring the stable operation of sensitive circuitry. Furthermore, it distributes power uniformly across the SLRs and facilitates clocking and configuration connections while also contributing to thermal management. At the chip level, the PDN forms a complex passive network that delivers power to each computing unit via the silicon interposer. The power supply transitions through interconnects between the package and the interposer layer before being locally distributed by the die power grid, an irregular, multi-layer metal mesh that connects to lower-level digital circuits.

C. Coupling Effect Between SLRs

The coupling effect in 2.5-D integrated systems occurs due to shared resources, such as the PDN and interposer, which interconnect multiple SLRs. This effect is driven by both power and electromagnetic interactions. Variations in power consumption by one SLR induce fluctuations in the shared PDN, creating voltage and current perturbations that propagate across the interposer and impact neighboring SLRs. These fluctuations result from the resistive, capacitive, and inductive characteristics of the PDN, including mutual inductance and parasitic capacitance in the closely spaced power and ground planes, vias, and traces. Additionally, the switching activity in one SLR generates alternating electric and magnetic fields that can couple into adjacent SLRs through electromagnetic interference. These electromagnetic coupling signatures, while enabling SLRs interaction and optimization, also serve as reliable indicators for tamper detection and system security by revealing anomalies in power or electromagnetic behaviors [7].

D. Delay-based On-Chip Sensor

It has been shown in multiple cases that the voltage fluctuations due to computation on the IC’s die could be measured with delay-based circuits placed on the same die [8]. Power consumption alteration affects the propagation delays of electrical signals. Such change in propagation delay can be recorded in on-die sensory circuits, such as ring oscillators [9] and time-to-digital converters (TDCs) [8]. These sensors have been used to detect voltage, electromagnetic (EM), and laser glitching and radiating attacks on FPGAs [10], [11]. However, they have not been used for integrity checks on multi-chip or chiplet systems. Implementation of RO-based sensors incurs high power usage, and they perform poorly for accurate

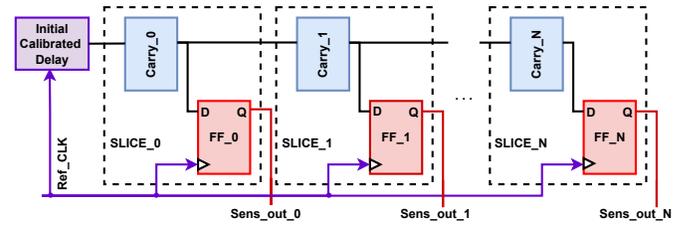


Fig. 3: high-level implementation of a TDC-based fault detection sensor

sensing (picosecond granularity). Therefore, in this paper, we utilize TDC sensors for our integrity-checking framework.

In this work, inspired by the TDC implementation described by Gnad et al. [12], we re-purpose a TDC design for integrity check purposes on multi-die FPGAs. Fig. 3 depicts a high-level implementation of the employed TDC. As highlighted, the sensor’s core components include an initial delayed signal, a tapped delay line, and corresponding output registers. The calibration process is necessary for the TDC sensors and is performed offline by adjusting delay elements (e.g., CARRY4) or by modifying the chain of combinational logic blocks. This process ensures the sensor’s output reaches a metastable state suitable for accurate sensing of tiny voltage fluctuations. The delay line typically employs fast carry propagation logic, physically constrained to form a sequential delay chain. Each delay unit’s output is propagated to an output register clocked by the original signal, with the binary sensor output determined by the propagation delay at each register’s input. Ideally, an external high-speed sampling circuitry is deployed to record the output of the TDC sensors. In this work, we organize a 2D mesh of TDC sensors on the verifier chiplet and perform a high-speed sampling on all TDCs simultaneously.

III. CHIPLETQUAKE

Considering the recent concerns regarding the potential chiplet-based security threats [13], defense against such threats requires run-time and an accurate integrity-checking mechanism in place. Motivated by the capacity of the shared PDNs in chiplet-enabled systems and the existing research for inter-chiplet fingerprinting [6], we develop a digital monitoring system to sense the impedance fluctuations of the physical environment of the chiplets. We present CHIPLETQUAKE to detect tiny and passive alterations in the interposer, as well as neighboring chiplets, which can serve as a verification framework to identify Hardware Trojans (HT).

A. High-level Design

Fig. 4 shows the high-level design of *ChipletQuake*. As shown, the verifier chiplet is equipped with some internal components of a monitoring system. With the use of a digitally designed frequency sweeper, an array of power waster circuitry is activated by oscillating on certain frequencies. We refer to these elements (e.g., inverter chains) as *Actuator Array*. Due to the shared PDN in the system, neighboring chiplets undergo frequency-dependent current and voltage fluctuation. At the

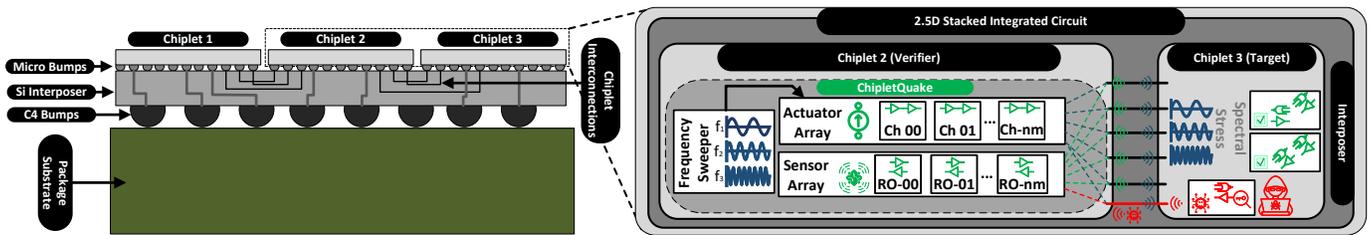


Fig. 4: High-level overview of CHIPLETQUAKE functionality

same time, another sensory circuit in *ChipletQuake* records this fluctuation by accurately sensing the voltage via digital delay-based or ring oscillator-based sensors.

During the monitoring routine, if the verifier identifies any noticeable deviation from the valid existing measurement (golden model) on the sensed values, it considers a possible malicious hardware alteration on the neighboring chiplets or as shown on the interposer itself.

B. Chiplet Verification Flow

To facilitate a reliable hardware-level integrity check, we develop a verification protocol that utilizes a challenge-response authentication scheme [14]. Instead of conventional digital signatures, a specific estimation of circuit impedance is considered as the response (signature). As illustrated in Fig. 5, the verifier chiplet deploys a 2D array on its reconfigurable fabric (e.g., FPGA). Inside each element of the array located in the chiplet layout, a sensor (e.g., TDC) is implemented, which is highlighted as a filled \blacktriangleright if enabled during the verification process.

Furthermore, elements of the arrays are also equipped with a current actuator illustrated as a filled \bullet once activated. Consequently, the verifier organizes a 2D grid of sensors and power wasters.

To extract a proper impedance-based signature as the golden model, the verifier first chooses a set N frequencies $\{Freq_N\} = \{f_0, f_1, f_2, \dots, f_{N-1}\}$ in which the impedance is estimated during the verification process. Then, by choosing a set of corresponding IDs in the grid, K actuator elements are selected. For instance in Fig. 5, actuators from the regions $\{Actuators\} = \{AC_0, AC_3, AC_6\}$ are selected and highlighted. These actuators are then activated and fed with the selected frequencies from $\{Freq_N\}$ set. At the same time, the verifier selects another set of M IDs, which are associated with the sensors that are responsible for recording the voltage-based fluctuations. As a simple example in Fig. 5, $\{Sensors\} = \{S_0, S_1, S_3, S_5\}$ are chosen.

Performing the entire verification process locally on the verifier chiplet requires the verifier to store all the golden signatures on the verifier chip. However, due to the possibility of storage limitation, the large size of multiple golden signatures makes this approach infeasible in some cases. Furthermore, to comply with the requirements of remote attestation scenarios [15], the integrity check should provide guarantees for remote users. In this case, a large attack

surface should be considered. Specifically, reply attacks on the signatures can bypass the verification process. Furthermore, dynamic reconfiguration of the target chiplets can affect the extracted signatures captured by the verifier. To overcome such challenges, *ChipletQuake* provides a one-time authentication protocol by utilizing a one-time verification key K_{ver} as the challenge for the target adjacent chiplets and the interposer itself. The verification key is generated by randomly selecting sets of IDs of the *Actuators*, *Sensors*, and the target *Frequencies* for the impedance sensing. Our experiments aligned with the previous studies show that each combination of the $\{K_{ver}\} = \{\{Act\}_K, \{Sen\}_M, \{Freq\}_N\}$ yields a unique impedance profile which then can be post-processed to represent a valid golden signature.

After recording multiple numbers of golden impedance signatures using different $\{K_{ver}\}$ s, the target device in the field can be tested on demand. The traces extracted from the verification process can be easily validated remotely. Note that, during the test process, the traces extracted from the chip's environment are a function dependent on $\{K_{ver}\}$ (which protects the security of the authentication protocol) and the physical layout and state of the hardware circuitry. Hence, any malicious hardware-level modification on the system in a package can be detected by analyzing the captured traces.

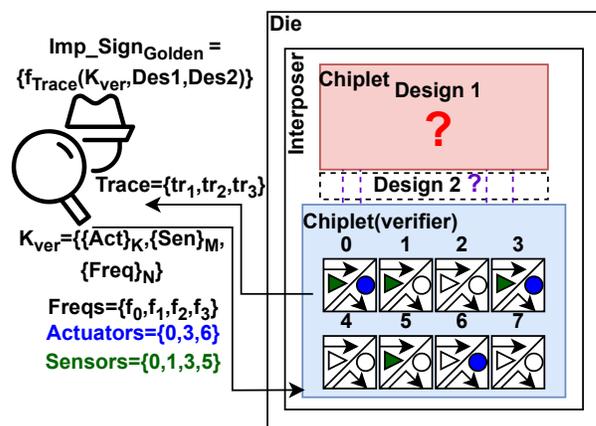


Fig. 5: Chiplet Verification Flow via Impedance Estimation

C. Frequency Band Selection

A PCB's power and ground planes form a cavity that can resonate at specific frequencies, occurring when the electrical

dimensions of the PCB align with integer multiples of the electromagnetic wavelength. At these resonant frequencies, the impedance of the PCB becomes more sensitive due to the interaction of interconnect parasitic inductance, parasitic capacitance, and decoupling capacitance. This intensified sensitivity makes the PCB more susceptible to even small changes in the impedance, such as those caused by a hardware Trojan and tampering events. These small changes can introduce additional parasitics or alter signal pathways, potentially leading to observable performance anomalies.

Additionally, at resonant frequencies, electromagnetic energy tends to concentrate in certain regions of the PCB. This localized accumulation of energy creates areas where the presence of a hardware Trojan can have a significant impact. A Trojan embedded in such regions may interact with the concentrated electromagnetic fields, leading to detectable deviations in signal integrity, power distribution, or electromagnetic emissions [16]. The resonant frequency of a rectangular cavity resonator can be derived from the following equation:

$$f_r = \frac{1}{2\pi\sqrt{\mu\epsilon}} \cdot \sqrt{\left(\frac{m\pi}{a}\right)^2 + \left(\frac{n\pi}{b}\right)^2 + \left(\frac{p\pi}{d}\right)^2} \quad (1)$$

where a and b are the cross-sectional sizes, and d is the length of the cavity while ϵ and μ are permittivity, and permeability of the material that cavity filled with it, respectively [17].

Knowing the physical dimensions of the target PCB and its relative permittivity, the fundamental resonate frequencies can be estimated for measurements.

D. Implementation Layout

To implement *ChiptletQuake*, it is vital to properly carry out the physical placement of the underlying blocks. Specifically, we make physical constraints on the chiptlet’s fabric to ensure that sensors and actuators are evenly distributed and deployed. Fig. 6 shows an implementation layout of *ChiptletQuake* with 32 monitoring blocks on an FPGA chiptlet. As mentioned, each block comprises a TDC sensor and an inverter-based actuator. Separated physically, each of these elements is controlled individually by a controller and can be configured to operate in different modes. Specifically, the sampling rate of the sensors, input frequency of the actuator chain, and sensing time interval can be remotely configured as parameters during the verification procedure.

IV. CASE STUDIES

A. Threat Model

The modern chiptlet architectures necessitate the design teams to integrate or procure chiptlet intellectual property (IP) from external vendors. However, it is impractical for these design teams to be directly involved in the development of every individual chiptlet. Consequently, organizations that outsource chiptlet components must depend on the manufacturers of these chiptlets to deliver reliable hardware unless robust security measures are implemented. In such a horizontal supply chain,

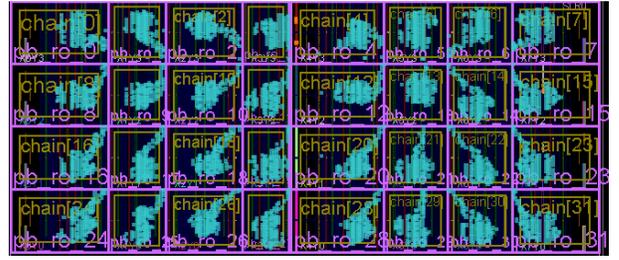


Fig. 6: CHIPLETQUAKE FPGA implementation layout with an array of 32 monitoring blocks

to guarantee the quality and integrity of the products, outsourcing companies should adopt a Zero-Trust security model where no inherent trust is granted to devices or users, network environment, or ownership [18]. Applying a Zero-Trust approach demands the verification of all chiptlet hardware, regardless of its source. Key vulnerabilities in chiptlet-based systems include risks such as hardware tampering, unauthorized probing, and the insertion of hardware Trojans. Given the extensive and global nature of the chiptlet supply chain, authentication is critical to ensure that each chiptlet meets the required standards and specifications.

To address these challenges, our fingerprinting method ensures the authenticity of the adjacent chiptlets and the host interposer by exploiting digital impedance estimation. Furthermore, existing authentication mechanisms depend on keeping the challenge-response pair secure from adversaries, which requires that the key itself is stored within a trusted environment. However, in the proposed method, the physical characteristics of the hardware account for the authenticity of the target hardware. Hence, any malicious tampering with the hardware yields an invalid key impeded in the impedance profile.

In our threat model, we consider multi-chiptlet system where a single challenger chiptlet verifies the integrity of the adjacent chiptlet and the interposer. We assume no access to target chiptlets in terms of logical challenge/response authentication. Moreover, our threat model requires the verifier to store post-silicon golden signatures prior to the test procedure. Furthermore, note that our treat model does not require the target chiptlet circuitry to be activated in terms of transistor switching activity. This is a particularly useful model for detecting dormant and evasive hardware Trojans, which are often implemented via tiny units.

B. Experimental Scenarios

We organize different case studies to thoroughly investigate the detection capability of the purposed digital impedance sensing in chiptlet-based FPGAs. Particularly, in this work, we focus on four distinct case studies for chiptlet verification. Fig. 7 highlights a high-level illustration of how each of these case studies is designed. As shown, in each of the scenarios, we deploy our verification hardware in chiptlet-0 (SLR0) and perform verification for chiptlets/interposers. We first study the case where different hardware modules are implemented in

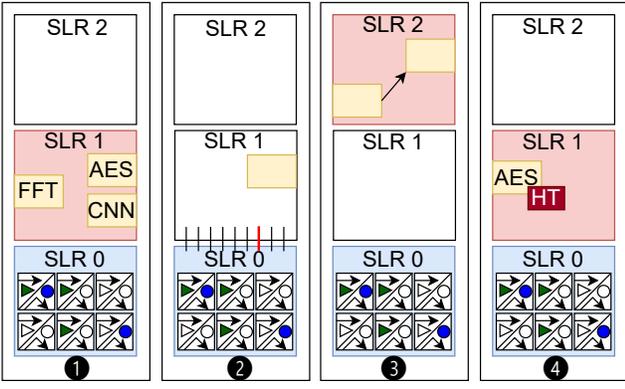


Fig. 7: High-level illustrations of the evaluation case studies

the adjacent SLR in ①. Here, we capture the impedance estimation for three hardware applications individually, and then we investigate if each of these hardware modules create a distinguishable fingerprint that can be detected by our sensors in the SLR0.

In ②, we study if modifications on the host interposer can be effectively detected. For this aim, we modify the utilization of communication lines between two chiplets. These lines are implemented and placed on the host interposer in the FPGA. The scenario here emulates the attacks that include interposer tampering and probing. For the ③ scenario, we further investigate the sensitivity of our framework for far chiplets. Specifically, we consider changing the placement of a single IP in SLR2 and monitoring the estimated profile on the verifier. Finally, in ④, we investigate if tiny hardware Trojans can be detected in adjacent chiplets.

V. EVALUATION RESULTS

A. Implementation Setup

For our evaluation, we used AMD Virtex™ UltraScale+™ VU37P HBM FPGA with 8GB of HBM DRAM memory. The target FPGA in this evaluation kit is XCVU37P-L2FSVH2892E, which includes three programmable FPGA chiplets (i.e., SLRs) and corresponding HBM DRAM chiplet. In our evaluations, we implement *ChipletQuake* on SLR 0 as the verifier and perform the integrity/verification tests for other SLRs. Furthermore, the device is connected via a UART serial connection to the controller computer that receives the traces and generates the signature.

B. Evaluation Metrics

As a commonly used metric in the hardware security domain, we chose Welch’s *t-test* [19] as the basic distance metric for our evaluations. For Welch’s *t-test*, small *p* values yield to reject the null hypothesis of similar (normal) distributions in distinguishability tests. For the sake of simplicity, it is best practice to usually select a threshold of $|t| > 4.5$ to reject the null hypothesis without considering the degree to conclude that the sets were drawn from different populations [20].

Nevertheless, as the impedance profile distribution might not necessarily follow a Gaussian trend in some cases, we also include the distribution-agnostic Wasserstein metric [21] to carry out distinguishability tests. The Wasserstein metric is the function that provides the distance between two probability distributions, each extracted from impedance estimation via *ChipletQuake*. The p^{th} ($p \geq 1$) Wasserstein distance between γ_i and τ_i is given by

$$W_p(\gamma_i, \tau_i) = [\inf \mathbb{E}(d(Im_i^G, Im_i^T))^p]^{(1/p)} \quad (2)$$

where $\mathbb{E}(Im)$ is the expected value of a random variable Im (estimated Impedance in this case), d is the Euclidean distance between two points, and the infimum is taken over all joint distributions of the random variables Im_i^G and Im_i^T with PDFs γ_i and τ_i , respectively.

C. Profiling Different Hardware Designs

As for our first set of experiments (Case Study ①), we simply collect three sets of traces of $T = 500$ for three hardware applications. Specifically, we consider AES, FFT, and a simple CNN, and then we calculate the average distance of the TDC sensed values with respect to a reference design on SLR1. Fig. 8 plots the average distance for each of these designs on the frequency point where the actuators were activated.

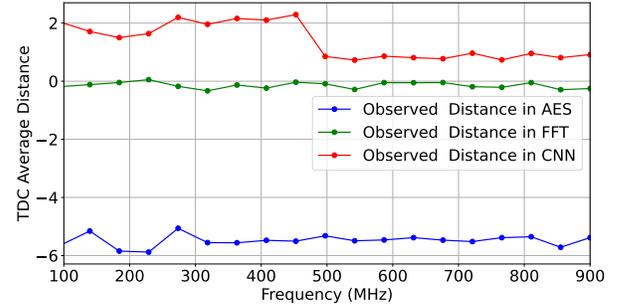


Fig. 8: TDC average distance on $T = 500$ traces for different configurations

D. Detecting Interposer Tampering

To verify the integrity of the interposer in our experiments, we generate two identical logical RTL hardware on SLR 1 as shown in ② in Fig.7. To emulate the interposer tampering, we set a different number of interposer-built SLL interconnections in each design to change the interposer utilization layout. Specifically our designs employ 129 and 133 SLLs between SLR 0 and SLR 1. Similar to the procedure we took for HT detection, we collect three sets of traces ($T = 1000$ for each set), including reference golden traces. Fig. 9 and Fig. 10 illustrate the *t-test* score for each of these two designs and the reliability reference score over the span of a selected frequency, respectively.

Furthermore, we calculate a null hypothesis threshold in each frequency point based on the Wasserstein distance. For Wasserstein distance, the null distributions are generated by

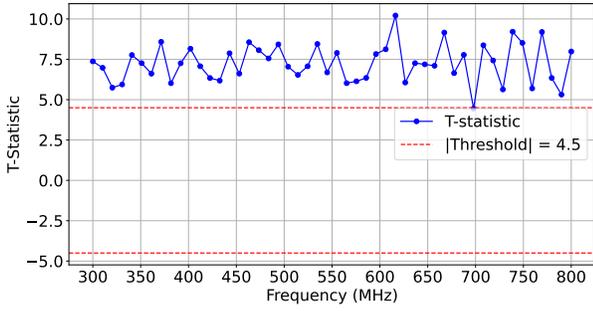


Fig. 9: T-test on $T = 1000$ traces for SLL129 Vs SLL133

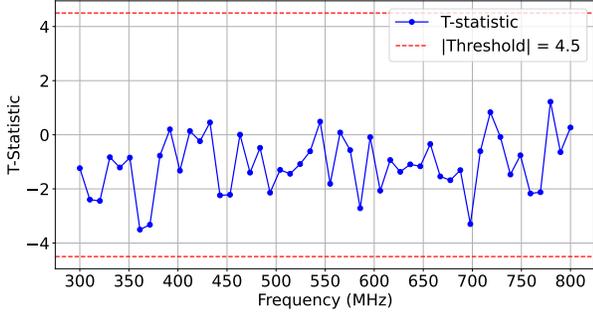


Fig. 10: T-test on $T = 1000$ traces for SLL129 Vs SLL129-Ref

performing 1000 bootstrap sampling with respect to the reference set. We set the significance value to p -value = 0.01 to estimate the threshold for rejecting the null hypothesis. Fig. 14 highlights the Wasserstein distance for interposer modification based on SLL utilization.

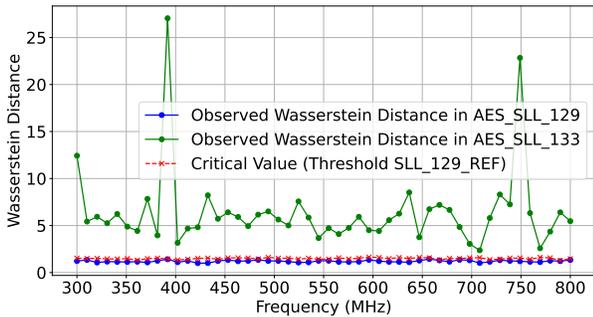


Fig. 11: Wasserstein distance on $T = 1000$ traces for AES-SLL129 Vs SLL133

E. Footprinting Further SLRs

Illustrated in ③ in Fig.7, for this experiment, we implement a test hardware design on SLR2, which is fabricated at a farther distance from the verifier deployed on SLR0. We collect two sets of $T = 500$ traces (and an additional reference set), where each set is associated with the same design in terms of functionality but routed differently in terms of implementation on the SLR2. We refer to these designs as $config_1$ and

$config_2$. Fig. 12 and Fig. 13 showcase the t-test score for each of these two designs and the reliability reference score over the span of a selected frequency, respectively.

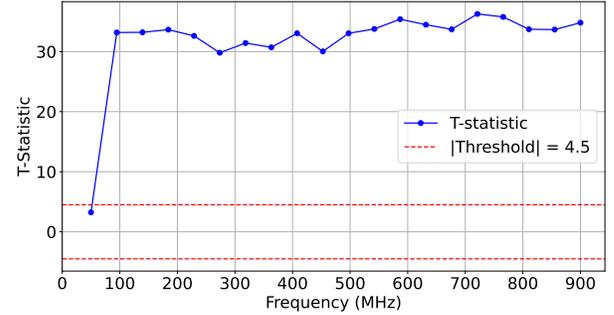


Fig. 12: T-test on $T = 500$ traces for $config_1$ Vs $config_2$ at SLR2

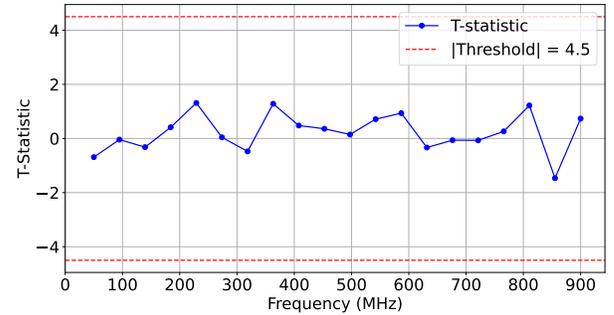


Fig. 13: T-test on $T = 500$ traces for $config_1$ Vs $config_1$ -Ref On SLR2

Moreover, Fig. 14 highlights the Wasserstein distance for between $config_1$ and $config_2$ with the $config_1$ as the reference.

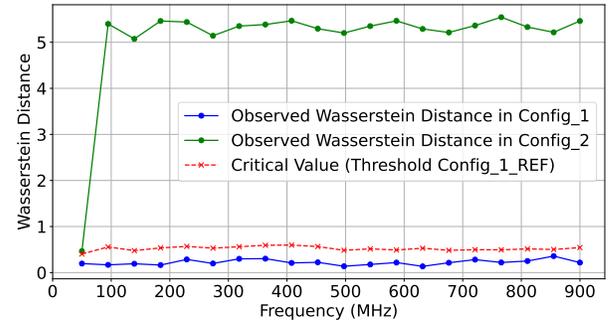


Fig. 14: Wasserstein distance on $T = 500$ traces for $config_1$ Vs $config_2$ On SLR2

F. Detecting Hardware Trojan

In our final set of experiments, as highlighted in ④, we evaluate *ChipletQuake* against the implementation of Hardware Trojans. For this case study, we utilized the Register-Transfer Level (RTL) HT benchmarks of AES implementations from Trust-Hub [22]. The original HT-free design in

these implementations is an AES-128 block cipher IP, with an 11-stage pipeline to perform the ten stages of AES encryption on the 128-bit block. For the HT implementation, we used AES-T1100 variation with an HT payload that modulates AES activity to create a power consumption pattern that leaks the AES key. We deployed each of these implementations on *SLR 1* and performed a distinguishability test from the verifier on *SLR 0* empowered by *ChipletQuake*.

For our experiment, we collect three sets of traces of $T = 500$, a set of traces for the legit *AES_HT_FREE* hardware as the reference, another set of traces for *AES_HT_FREE* for testing, and a set of malicious *AES_HT* implementation.

Fig. 15 shows the frequency-based T-test distinguishability results captured for two sets of experiments where *AES_HT_FREE* and *AES_HT* are implemented in the adjacent *SLR 1*.

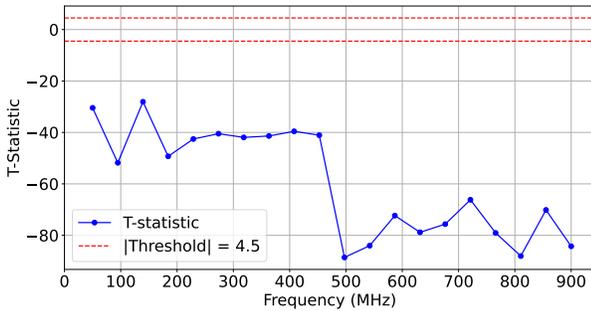


Fig. 15: T-test on $T = 500$ traces for AES-HT-Free Vs AES-HT

Furthermore, to showcase the reliability, we perform another set of HT-Free impedance estimation and compare it to the existing HT-Free reference traces. Fig. 16, depicts the T-test for two sets of identical implementation of HT-free AES. As anticipated, we can verify the difference score is confined within the $|t| < 4.5$ similarity range.

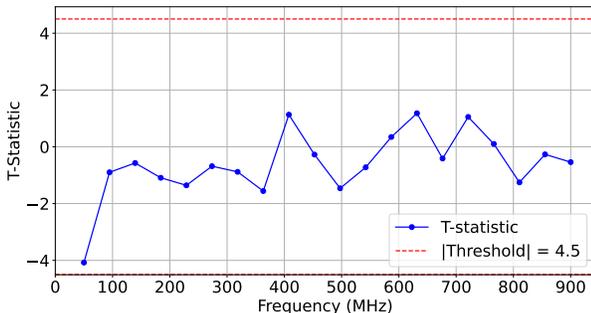


Fig. 16: T-test on $T = 500$ traces for AES-HT-Free Vs AES-HT-Free-Ref

As shown in Fig. 17, the calculated Wasserstein distance of the HT-included IP is visible by a large margin, and hence malicious circuit on the chiplet can be detected effectively.

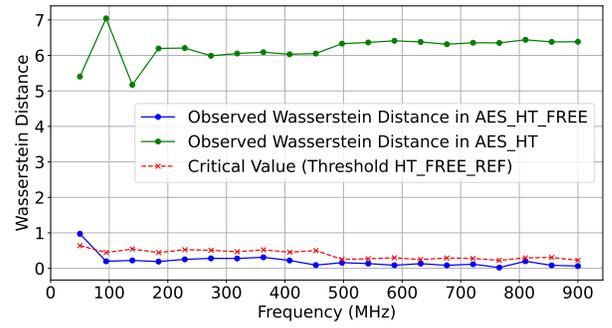


Fig. 17: Wasserstein distance on $T = 500$ traces for AES-HT-Free Vs AES-HT

VI. DISCUSSIONS

A. Comparison to Related Works

Power-based side-channel attacks have been shown to be effective in chiplet-based systems to extract information from adjacent chiplets. In this regard, similar approaches such as [3] can be used to detect anomalies in adjacent chiplets. Such works exploit the alteration sensed in power consumption of the neighboring chiplets due to the dynamic execution of the target circuits. Hence, static and dormant malicious circuits (e.g., HTs) are not effectively discovered unless activated.

There have also been similar works to utilize sensors in chiplets for verification and protection in SiP. Specifically, authors in [6] use the impedance estimation via FFT to fingerprint the chiplets. Although similar actuator/sensor architecture can be used to estimate impedance via voltage fluctuations, time-to-frequency conversion via FFT potentially drops the SNR required for intra-SLR fingerprinting.

Our work presents a frequency domain sweeping approach that provides a rich profile of impedance that can be processed to identify static circuits which are not required to be dynamically activated. Such methodology presents enough accuracy to detect tiny static dormant HTs.

B. Further Applications

It might be possible to use this framework to perform dynamic verifications as well. This means that the signature procedure can be performed during the switching activities of the adjacent chiplet. The impedance-based dynamic fingerprinting potentially opens up the possibility of carrying out adversary side-channel attacks on the neighboring chiplets. Furthermore, as another application, it is also possible to perform extensive templating/profiling to fingerprint a target IP in threat models that physical side-channels are considered.

VII. CONCLUSION

The transition to chiplet-based designs addresses critical challenges in modern semiconductor manufacturing but also introduces significant security vulnerabilities in the hardware supply chain. This paper presented *ChipletQuake*, a framework for post-silicon verification of physical security in chiplet-based systems. By leveraging impedance sensing of the power

delivery network (PDN), *ChipletQuake* effectively detects tampering events in the interposer and neighboring chiplets without requiring additional hardware. The impedance estimation method is able to detect dormant, static, and tiny modifications on the MCMs. Our experimental results demonstrate its capability to identify hardware Trojans and interposer tampering, validating its effectiveness in enhancing the security of FPGA-based chiplet systems.

REFERENCES

- [1] A. Deric and D. Holcomb, "Know time to die—integrity checking for zero trust chiplet-based systems using between-die delay pufs," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 391–412, 2022.
- [2] A. Deric, K. Mitard, S. Tajik, and D. Holcomb, "Evaluating vulnerability of chiplet-based systems to contactless probing techniques," *arXiv preprint arXiv:2405.14821*, 2024.
- [3] T. Zhang, M. L. Rahman, H. M. Kamali, K. Z. Azar, and F. Farahmandi, "Sipguard: run-time system-in-package security monitoring via power noise variation," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2023.
- [4] M. O. Hossen, A. Kaul, E. Nurvitadhi, M. D. Pant, R. Gutala, A. Dasu, and M. S. Bakir, "Analysis of power delivery network (pdn) in bridge-chips for 2.5-d heterogeneous integration," *IEEE Transactions on Components, Packaging and Manufacturing Technology*, vol. 12, no. 11, pp. 1824–1831, 2022.
- [5] T. Mosavirak, S. K. Monfared, M. S. Safa, and S. Tajik, "Silicon echoes: Non-invasive trojan and tamper detection using frequency-selective impedance analysis," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2023, no. 4, pp. 238–261, 2023.
- [6] H. Zhu, W. Cao, and X. Zhang, "Pdnsic: Identifying multi-tenant cloud fpgas with power distribution network-based signatures," in *2023 IEEE/ACM International Conference on Computer Aided Design (ICCAD)*. IEEE, 2023, pp. 1–8.
- [7] I. Giechaskiel, K. Rasmussen, and J. Szefer, "Reading between the dies: Cross-slr covert channels on multi-tenant cloud fpgas," in *2019 IEEE 37th International Conference on Computer Design (ICCD)*. IEEE, 2019, pp. 1–10.
- [8] M. Zhao and G. E. Suh, "Fpga-based remote power side-channel attacks," in *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 229–244.
- [9] J. Gravellier, J.-M. Dutertre, Y. Teglia, and P. Loubet-Moundi, "High-speed ring oscillator based sensors for remote side-channel attacks on fpgas," in *2019 International conference on ReConFigurable computing and FPGAs (ReConFig)*. IEEE, 2019, pp. 1–8.
- [10] M. A. Kajol, S. Sunkavilli, and Q. Yu, "Ahd-lam: A new mitigation method against voltage-drop attacks in multi-tenant fpgas," in *2023 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*. IEEE, 2023, pp. 1–6.
- [11] S. K. Monfared, K. Mitard, A. Cannon, D. Forte, and S. Tajik, "LaserEscape: Detecting and Mitigating Optical Probing Attacks," in *2023 IEEE/ACM International Conference on Computer Aided Design (ICCAD)*, 2024.
- [12] D. R. Gnad, C. D. K. Nguyen, S. H. Gillani, and M. B. Tahoori, "Voltage-based covert channels using fpgas," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 26, no. 6, pp. 1–25, 2021.
- [13] S. Juan, A. Fady, P. Anthony, R. Philippe *et al.*, "On hardware security and trust for chiplet-based 2.5 d and 3d ics: Challenges and innovations," *IEEE Access*, 2024.
- [14] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "Pycra: Physical challenge-response authentication for active sensors under spoofing attacks," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, pp. 1004–1015.
- [15] G. Coker, J. Guttman, P. Loscocco, A. Herzog, J. Millen, B. O'Hanlon, J. Ramsdell, A. Segall, J. Sheehy, and B. Sniffen, "Principles of remote attestation," *International Journal of Information Security*, vol. 10, pp. 63–81, 2011.
- [16] Y. Han, X. Wang, and M. Tehranipoor, "Cipa: Concurrent ic and pcb authentication using on-chip ring oscillator array," in *2018 IEEE 27th Asian Test Symposium (ATS)*. IEEE, 2018, pp. 109–114.
- [17] S. Ramo, J. R. Whinnery, and T. Van Duzer, *Fields and waves in communication electronics*. John Wiley & Sons, 1994.
- [18] V. Stafford, "Zero trust architecture," *NIST special publication*, vol. 800, p. 207, 2020.
- [19] B. Bilgin, B. Gierlichs, S. Nikova, V. Nikov, and V. Rijmen, "Higher-order threshold implementations," in *Advances in Cryptology—ASIACRYPT 2014: 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, ROC, December 7-11, 2014, Proceedings, Part II 20*. Springer, 2014, pp. 326–343.
- [20] T. Schneider and A. Moradi, "Leakage assessment methodology: A clear roadmap for side-channel evaluations," in *Cryptographic Hardware and Embedded Systems—CHES 2015: 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings 17*. Springer, 2015, pp. 495–513.
- [21] M. Arjovsky, S. Chintala, and L. Bottou, "Wasserstein generative adversarial networks," in *International conference on machine learning*. PMLR, 2017, pp. 214–223.
- [22] Trust-Hub, "Hardware Trojan Benchmarks," [Online]<https://trust-hub.org>, 2025.