ToSHI - Towards Secure Heterogeneous Integration: Security Risks, Threat Assessment, and Assurance

Nidish Vashistha, Md Latifur Rahman, Md Saad Ul Haque, Azim Uddin, Md Sami Ul Islam Sami, Amit Mazumder Shuo, Paul Calzada, Farimah Farahmandi, Navid Asadizanjani, Fahim Rahman, and Mark Tehranipoor
Florida Institute for Cybersecurity (FICS) Research, Department of Electrical & Computer Engineering,
University of Florida, Gainesville, 32611, FL, USA

***Abstract*—The semiconductor industry is entering a new age in which device scaling and cost reduction will no longer follow the decades-long pattern. Packing more transistors on a monolithic IC at each node becomes more difficult and expensive. Companies in the semiconductor industry are increasingly seeking technological solutions to close the gap and enhance cost-performance while providing more functionality through integration. Putting all of the operations on a single chip (known as a system on a chip, or SoC) presents several issues, including increased prices and greater design complexity. Heterogeneous integration (HI), which uses advanced packaging technology to merge components that might be designed and manufactured independently using the best process technology, is an attractive alternative. However, although the industry is motivated to move towards HI, many design and security challenges must be addressed. This paper presents a three-tier security approach for secure heterogeneous integration by investigating supply chain security risks, threats, and vulnerabilities at the chiplet, interposer, and system-in-package levels. Furthermore, various possible trust validation methods and attack mitigation were proposed for every level of heterogeneous integration. Finally, we shared our vision as a roadmap toward developing security solutions for a secure heterogeneous integration.**

***Index Terms*—Hardware Security & Assurance, Secure Heterogeneous Integration, Semiconductor Supply Chain, Chiplet and Trusted Microelectronics.**

I. Introduction

ELECTRONIC devices are becoming deeply ingrained in our lifestyle by transforming the way we live and work. We live in a digital economy with the widespread connectivity of high-speed devices generating big data. At the same time, some systems need to capture, store, and analyze this big data to process further transactions (autonomous cars, data centers, and AI-based systems). This data evolution is supported at the ground level by state-of-the-art semiconductor ICs that provide multiple processing cores, high bandwidth memory, and high-speed I/O ports. These advanced ICs are available because of Moore's law, pushing the semiconductor industry to supply faster, smaller, and cheaper semiconductor ICs. However, this law is ending due to the fabrication cost, power dissipation, and yield issues at advanced technology nodes. The ITRS 2015 has set a long-term vision to sustain the historical scaling of CMOS technology to keep Moore's law alive by using Heterogeneous Integration (HI) [1]. The HI refers to integrating individually designed, and fabricated components that can be assembled on a substrate layer called an interposer to perform a function like an SoC.

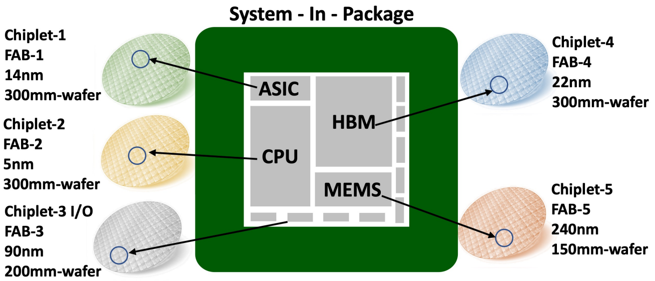


Figure 1: Heterogeneous integration to build a SiP

Heterogeneous integration combines (see Figure 1) separately manufactured components of different technology nodes and functionality to form a higher-level assembly called System in Package (SiP) [1] or Multi-Chip Module (MCM). A SiP provides greater functionality and achieves better-operating characteristics which are challenging to achieve on a single die system-on-chip (SoC). In a SiP, components such as chiplets, MEMS devices, and active/passive parts are integrated into a single package. A chiplet is an individually fabricated silicon die (also known as hardened IP) for a targeted function such as memory, analog-mixed signal, RF, or processor. The system-in-package can be a vertical stacking (3D) or adjacent placement (2.5D) of chiplets on the substrate layer called an interposer. Several integrated device manufacturers (Intel, Micron, and Samsung), fabless design houses (AMD and IBM), foundries (TSMC), and outsourced semiconductor assembly and testing companies (TSMC and Amkor) are working on developing heterogeneous integration solutions. For example, Intel Agilex and the AMD EPYC are the commercially available heterogeneous 3D system-in-packages (SiP). DARPA has a similar vision for the US government's DoD application designs and technologies through the Common Heterogeneous Integration and IP Reuse Strategies (CHIPS) program for trusted microelectronics.

Despite the many lucrative advantages of HI, it requires further research and development, including packaging technology, standardization of interconnecting interfaces, commu-

This work is partly sponsored by the Office of Naval Research (ONR) under grants N00014-21-1-2513 and N00014-22-1-2560. For correspondence, please reach out to both authors nidish@ufl.edu and tehranipoor@ece.ufl.edu.

[1] In a real sense, SiP is a couple of decade-old technology developed to shrink PCBs and achieve higher bandwidth and lower power. However, these days, the SiP term is re-used for marketing purposes as a synonym for heterogeneous integration (HI). In this paper, the term SiP stands for packages made through HI technology.

nication protocols, and secure design. For example, the packaging methods should consume less space to support small form factors. In addition, the design of the interconnecting interface of chiplets must conform with the speed, power requirements, and crosstalk issues. Some organizations (ODSA and CHIPS Alliance) are independently developing Die-to-Die interface protocols such as Advanced Interface Bus (AIB), Bunch of Wires (BoW), and open High Bandwidth Interconnect (openHBI). Recently, leaders in semiconductors design, packaging, IP suppliers, foundries, and cloud service providers have formed a consortium to develop an open standard for interfacing chiplets, i.e., Universal Chiplet Interconnect Express (UCIe) [2]. However, this interface standard's security vulnerabilities and associated risks are yet to be evaluated.

Like SoCs, the SiPs can be vulnerable to hardware security attacks. Hence, there is a need for trust validation of chiplets, substrate layer/interposer security, and security assessment of SiPs. In the SiP supply chain, a SiP OEM or designer obtains necessary chiplets from different chiplet equipment/component manufacturers (OEMs/OCMs) with no information about the IPs design of these chiplets. Further, the horizontal business model renders offshore chiplet foundries to control the fabrication and testing of the chiplets. This business model further raises significant security concerns about the SiP's confidentiality, integrity, and availability (CIA) by making it vulnerable to various threats (e.g., hardware Trojans, out-of-spec, cloned, and overproduction). Therefore, a trust validation mechanism must be developed to validate the authenticity of chiplets acquired from different OCMs. In addition to trusted chiplets, the interposer layer should be free from any malicious changes (Interposer level Trojans) and immune to reverse engineering attacks.

Further, before deploying the SiP package in a system, a security assessment is required to ensure it is resistant to any security attacks. For example, similar to SoCs, a SiP package may be physically or remotely attacked (fault injection, contact-less probing, or side-channel analysis). In addition, a SiP designer needs to ensure secure communication between chiplets (anti-bus snooping or preventing unauthorized memory access) for a secure SiP. Hence, these security concerns should be addressed, from procurement of chiplets to interposer design & fabrication to the integration stage for a trusted & secure SiP.

To summarize, we propose a comprehensive three-tier (chiplet-to-interposer-to-SiP) and end-to-end hardware security approach for secure heterogeneous integration by identifying risk and threats at every level as depicted in Figure 4. Therefore our contributions are:

- We have analyzed the chiplet security problem by identifying risks, threats, and vulnerabilities by determining attack vectors and surface. Furthermore, we identified adversarial entities that can compromise chiplet security and suggested respective trust validation methods.
- We have investigated security vulnerabilities at the interconnect (interposer) level of heterogeneous integration with a comprehensive set of possible threats in the supply chain, followed by specified the associated attack vectors & surface and recommended possible countermeasures.
- We analyzed SiP level security for secure heterogeneous integration, including the attack surface, threat model, vulnerabilities, and potential countermeasure. The role of security policies in protecting on-chip assets is also discussed.
- A road map is proposed toward a secure heterogeneous integration for a trusted system-in-package design. This road map will assist the research community by opening multiple avenues for future research.

This paper primarily focuses on the secure heterogeneous integration of chiplets and is organized as follows: Section II briefly presents background about the fundamentals of heterogeneous integration and respective security challenges, which serves as a motivation for research. Then, section III presents the concept of chiplet security problems and trust validation methods. Interposer-level security threats are analyzed in Section IV with possible solutions. SiP level security problems are investigated, and security policies as potential solutions are discussed in Section V. Next, the research road map towards a secure heterogeneous integration is proposed in Section VI. Finally, we conclude in Section VII.

II. Preliminaries

A. Motivation for HI

Heterogeneous integration is expected to keep the pace of More-than-Moore (MtM) progress. It is moving forward with higher performance, yield, reduced latency, compact size, lighter weight, low power, and cost of semiconductor. Here are the prime motivations for the semiconductor industry to pace towards HI:

1) Features of Heterogeneous Integration: There are three primary drivers for innovation in heterogeneous integration, which can be seen as its critical features, presented by DARPA [3]:

- **Technological Diversity -** Heterogeneous integration involves using a variety of chiplets that can differ by technology node and foundry when integrated on the common interposer. For example, a 14nm transistor SRAM memory chiplet fabricated by foundry A can be integrated with a 22 nm-based processor chiplet fabricated by foundry B on the same interposer. This approach allows newer technology node chiplets to be integrated with older but high-yielding technology node chiplets, adding to this technological diversity of the system. This way, chiplets with their respective matured process nodes can be integrated into the same package.
- **Functional Diversity -** Another feature of heterogeneous integration is that chiplets with diverse functions can be integrated on the same package. For example, memory, logic chiplets, analog I/O, and MEMS sensor chiplets can be integrated on the interposer to design a SiP for an end-user application. These diverse chiplets perform specific and unique roles in the integrated SiP, allowing the modular and custom design of the SiP package.
- **Materials Diversity -** Heterogeneous integration also allows for diversity in the materials used to create these chiplets—the chiplet acts as a black box in the overall system. As long as the chiplet's materials do not affect the functionality of the integrated system in an unintended way, then the materials of each independent chiplet can

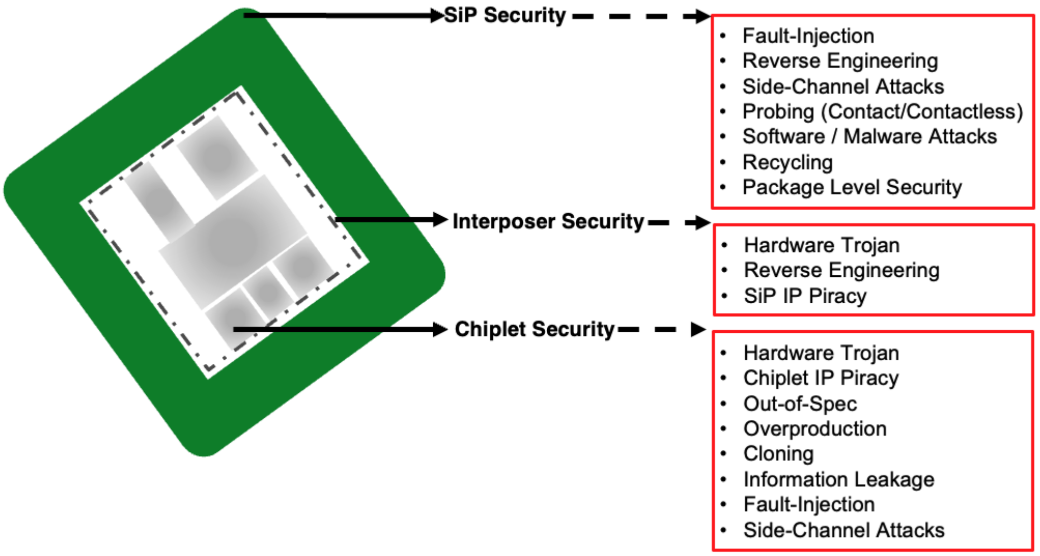


Figure 2: Possible identified security risk and threats at various levels of heterogeneous integration.

differ. Certain chiplets may be optimized for a specific function and have enhanced capabilities with newer materials.

2) The Continuation of Moore’s Law: Over the past half-century, Moore’s Law has been the guiding framework for predicting the direction of innovation in the semiconductor industry. This law pushes researchers to scale CMOS devices to double the density of transistors in an IC every two years. However, there is contention in the community as to whether this principle is becoming less apparent as further decreases in transistor size can lead quantum factors to become more relevant and increase manufacturing costs for these classical processes [4]. Revolutionary innovations, especially in packaging and design like heterogeneous integration, have enabled the viewing of Moore’s law with a new lens, using the functional density rather than scaling of transistor density as a predictor for performance.

3) Higher Yields with Lower Development Cost: Heterogeneous integration can lead to an overall increase in the yield of SiP due to the incorporation of known good dies (KGD) or chiplets, which can, in turn, be manufactured with a higher yield. Further technological advances have increased integration and stacking yields while decreasing manufacturing and research costs. Collective die-to-wafer bonding has been proposed even further to increase transfer bonding and electrical die yields [5]. Also, because chiplets are used from a matured process node, the development cost of SiP is reduced as post-silicon validation is rarely required. Previously researchers have demonstrated high yield and superior reliability manufacturing capability in high-performance 3D-ICs [6].

4) SiP for Better Performance: As performance gains by increasing transistor count per area on a die might be flat-lining, heterogeneous integration by incorporating various dies from different OEMs can enable higher performance by increased memory access speeds. For example, with 3D packaging technology, CPU and memory dies can be stacked, allowing increased memory bandwidth and decreased transmission latency as the dies have much shorter interconnects. [7]. Furthermore, 2.5D, 3D, and 5.5D packaging increase functional density as the dies are integrated into the same package, communicating through a silicon interposer and through silicon vias (TSV). The interposers are currently under research to increase their communication quality and rate with a reduction in overall thickness and complexity of the redistribution layer in the package. Active interposers are even being proposed where transistor-based logic circuits are embedded in the interposer, further increasing the functional density of the SiP.

5) Form Factor (Space/Size) Reduction: The 2.D and 3D packaging paradigms have led to smaller area and size requirements. The smaller size compared to traditional packaging can be attributed to integrating these various dies in one package rather than multiple separate dies connected using traces on a printed circuit board (PCB). Interconnects are, as a result, smaller in these integrated technologies, further increasing speed and decreasing power usage. 3D packaging gives the best functional density benefits as these dies are stacked vertically and horizontally. However, it introduces many thermal challenges, as these dies emit heat within the stack. 2.5D has also increased functional density compared to traditional packaging but has less functional density than 3D since chiplets are not vertically stacked but horizontally integrated.

Hence, HI can achieve a compact form factor by 2.5D and 3D packaging, increase performance, high manufacturer yields, and reduce overall area [8].

B. Challenges Towards RoadMap for HI

Although heterogeneous integration offers numerous advantages and sounds promising in the More-Than-Moore (MTM) approach, incorporating functionally diverse dies adds value to the SiP package but may not necessarily scale according to ”Moore’s Law.” In addition, various architectural design and security-related challenges need to be overcome while developing a system-in-package.

1) Interface Standards: One big challenge in SiP design is the interfacing of chiplets due to the variety of chiplets and I/O interfaces. Therefore, attempts have been made by mainstream SiP integrators to develop fast and simple chiplet-to-chiplet interfaces so that various types of chiplets can be connected. These efforts will eventually result in shorter SiP design and assembly time.

- **Serial Interfaces -** Based on transmission distance, the serial interface can be divided into the following categories long reach (LR), medium reach (MR), very short reach (VSR), extremely short reach (XSR), and ultra short-reach (USR) SerDes. LM/MR/VSR SerDes are used for inter-chip and chip-to-module communication in PCB boards. They are also used for PCIe, Ethernet, and Rapid I/O communicating interfaces. However, advantages like reliable transmission of these SerDes do not apply to heterogeneous integration areas, performance, and power. XSR SerDes accommodates the SerDes standard of Die-to-Die and Die-to-Optical engines. As the bandwidth increases, the power consumption and delay also increase. Compared to XSR, USR is suitable for high-speed interconnection in Die-to-Die communication via 2.5D and 3D packaging technologies. Ultimately, the transmission distance of USR hinders the large-scale integration of chiplets. [9]
- **Parallel Interfaces -** The common chiplet Die-to-Die communication interface for intel's AIB, EMIB TSMC's Low-voltage-In-Package-INterCONnect (LIPINCON), etc. Intel's AIB sends and receives data via microbumps from one chiplet to another. The benefit of a parallel interface, such as AIB, is that it has extremely low latency, power, and area requirements. The main disadvantage is that it necessitates using a silicon interposer or similar packaging technology, which adds significant cost [10].
- **Universal Chiplet Interconnect Express (UCIe) -** It is an open industry standard interconnect that provides chiplets with high-bandwidth, low-latency, power-efficient, and cost-effective on-package connectivity. It covers computation, memory, storage, and connectivity demands throughout the computing spectrum, including cloud, edge, corporate, 5G, automotive, high-performance computing, and hand-held segments. UCIe can package dies from various sources, including diverse fabs, designs, and packaging technologies. It is the first package-level integration that provides energy-efficient and cost-effective results. UCIe can be used in two different ways. First, as a memory, graphic accelerators, networking devices, modems, and other board-level components can be integrated at the package level, with applications ranging from hand-held devices to high-end servers, with dies from numerous sources coupled through different packaging methods even on the same package. The second application is to provide off-package connectivity using various types of media (e.g., optical, electrical cable, mmWave) and UCIe Retimers to transport the underlying protocols (e.g., PCIe, CXL) at the rack or even pod level. These protocols support resource pooling, resource sharing, and even message passing using load-store semantics to derive better power-efficient and cost-effective performance at data centers [2]. The latest UCIe 1.0 specification maps PCIe and CXL protocols natively as those are widely deployed at the board level across all computing segments. Therefore, it relies on the security solutions already deployed for the previously developed ones PCIe and CXL protocols. Furthermore, it is 'silent' about the security policies and methods a SiP designer can use for a secure system-in-package. Therefore, it may need further research to investigate vulnerabilities and incorporate security solutions in this standard.

2) Less Power: The SoCs' Performance-Per-Watt (PPW) design metric also holds for SiPs that use diverse functional chiplets. The SiP's ultimate objective is to provide the highest possible processing bandwidth at the cost of the lowest power consumption. The low PPW objective can save battery power in handled battery power devices. It can also reduce heating issues in constantly powered (car and data-centers) and battery-powered devices.

3) Thermal Management: Heterogeneous integration can increase the overall power density of the SiP, which can, in turn, increase total package power dissipation. However, power is generally dissipated as heat, and it can increase thermal cross-talk, and temperature-sensitive components need further thermal isolation [11].

4) Secure Heterogeneous Integration: During the last few decades, hardware security and trust assurance (free from any counterfeiting issues) has emerged as a vital parameter during circuit design and system development. After the emergence of various threats and vulnerabilities at the system level, the integrated circuits, PCB, and systems are now designed for security during their design phase. However, not many security assessments have been done on heterogeneous integration technology. For a secure heterogeneous integration, a bottom-up security approach is required from the root level (chiplets) to the packaging (interposer) to the final deployment (system) level.

- **Chiplet Security: Trust Validation of Chiplets -** A SiP designer must source trusted chiplets from various chiplet OEMs for heterogeneous integration. Like fabless packaged IC design companies, chiplet fabless OEMs will rely on pure-play overseas foundries for fabrication. These foundries have full access to GDSII, test patterns, and a confidential fabrication process beyond design houses' control. An adversarial foundry can insert malicious changes or hardware Trojan during the manufacturing of a chiplet. A chiplet with a Trojan inside a heterogeneous integration can expose that system-in-package to various attacks. For example, it can cause a denial of service (DoS) to cause reliability issues, Man-in-the-middle (MITM) attacks to get unauthorized access to confidential data such as encryption keys, and the bias of neural networks. For a secure heterogeneous integration, all chiplets need trust validation by the SiP designer.

  The trust validation of these chiplets can be very challenging for a SiP designer. They do not access proprietary information such as chiplet GDSII design and test patterns. Besides foundry, a chiplet design house cannot share the above-mentioned proprietary information with anyone in the supply chain. Finally, the chiplets are sold through various distributors, which cannot be trusted due to the involvement of an overseas foundry. In this trustless and IP confidentiality scenario, only the design house can validate the trustworthiness of the chiplets. Such trust validation steps require much effort in terms of time and money. Unfortunately, no universal standards or independent trust validation entities exist for chiplet security assurance.

- **Interposer Level Security: Secure Packaging -** With the insurgence of hardware-based attack reports and added attack vectors from various entities associated with heterogeneous integration, security assessment of packaging is crucial for hardware assurance of SIPs used in the military, space, and automobiles. The threat model exploiting the vulnerabilities pertinent to material and fabrication in IC packaging can be extended to SiPs. An adversary can alter the package material composition to cause chip failure during deployment. Unfortunately, current research trends for semiconductor packaging in industry and academia mainly focus on packaging reliability while its security is barely addressed. An adversarial integration facility can maliciously insert Trojans in an active interposer and alter packaging materials to create vulnerabilities in SiP that may be very difficult to detect in the post-manufacturing stages.

  The current process to assess packaging integrity primarily focuses on testing the chip's reliability during failure analysis and in-process testing. The physical inspection methods such as X-ray Photoelectron Spectroscopy (XPS), X-ray Fluorescence, Scanning Electron Microscopy, and Tera-Hertz Imaging can be effective for material composition analysis, interface anomalies, and malicious change detection [12], [13]. However, the effectiveness of these methods greatly depends on the complexity and material composition. For example, the sub-micron micro-bumps that connect the die and an interposer cannot be detected using a Scan Acoustic Microscopy (SAM). In addition, it may be challenging to detect without decapsulating the assembled SiP. Therefore, destructive detection techniques are required to provide robust integrity checks at the cost of time.

  For this reason, these checks are applied to random samples and cannot offer extensive hardware assurance. Existing methods may suffice to address the inherent process-induced reliability issues. However, new detection techniques are needed to ensure packaging integrity and provide hardware assurance.

C. Current Advancements in Heterogeneous Integration

This section will discuss the heterogeneous integration supply chain, applications, and secure design initiatives.

- **SiP Supply Chain -** As compared with SiP, SoC supply chains are straightforward due to fewer manufacturing steps and entities involved. However, the focus of SiPs has shifted from monolithic systems to the consumer-focused realm, where computing has become pervasive and increasingly heterogeneous. As a result, supply chain dynamics have inevitably become far more complex (see Figure 3).

  Recent trends and research illustrate the improvement of chiplet integration technology in heterogeneous systems, which necessitates the generation of a new business model and modification of the conventional supply chain of an SoC. In the SiP supply chain, an entity similar to the SoC integrator called SiP designer or OEM sources various chiplets for heterogeneous integration to develop custom silicon "chips" or system-in-packages. As the chiplet ecosystem evolves continuously to provide better system-level scaling, higher bandwidth communication, higher performance, higher functional and integration complexity, less power consumption with reduced development costs, and reduced time-to-market brackets, new entities are participating in the supply chain of the heterogeneous system. Chiplet OEMs (Fabless or IDMs), IP vendors, CAD tool developers, and pure-play foundries are the primary entities who control the availability of the chiplet in the supply chain to a great extent [14]. Chiplet OEMs with advanced research facilities and state-of-the-art design technology (e.g., Intel, AMD, Micron, Apple) have their chiplets in the market and high volume production.

  To achieve high computing performance at a reduced cost, AMD provides chiplets to the supply chain that includes multi-core processor dies, IO dies, and high bandwidth memory dies in different technology nodes. Intel has demonstrated its chiplet integration feasibility by designing high-performance, high-bandwidth heterogeneous systems by integrating an FPGA die and IO die with an AIB interface. AIB connections can be made using wires on an interposer and bridge technologies such as Intel's EMIB bridge [15]. Some start-up fabless semiconductor companies such as zGlue are trying to establish a set of basic EDA toolchains for chiplets. Some advanced packaging technologies (Substrate-based, Silicon Interposer-based, Silicon Bridge-based, and Redistribution Layer-based) have been exploited to achieve higher IO density with reduced transmission delay and power consumption in the heterogeneous integration of chiplets. TSMC has implemented substrate-based fanout packaging based on RDL in Apple's A10 processor to make it more cost-effective than silicon interposer-based packaging.

  Although the roadmap of the current chiplet supply chain demonstrates much advancement in its development and implementation, it raises some unique challenges that need to be resolved. The standardization of interface and communication protocols in the design stage of a chiplet must consider the new fabrication process, packaging technology, and integration technology to achieve flexibility and scalability [14]. The current chiplet design and integration technology requires comprehensive EDA tool support to reduce the failure in post-silicon analysis and improve the quality of the manufacturing process. Moreover, the security vulnerabilities of the chiplet supply chain have emerged from the entities that can be potentially untrusted such as 3PIP, untrusted chiplet OEMs (fabless design house or IDM), chiplet pure-play foundry (for fabless chiplet OEMs), chiplet integrator. A chiplet integrator can be a single entity providing complete integration (interposer design, packaging, assembly, and testing) or segregated into multiple separate entities, depending upon their expertise or business model. Finally, an adversarial end-user is the entity that procures a SiP package to perform unethical attacks on the in-field SiP package to exploit its vulnerabilities to violate the CIA triad or produce counterfeit packages.

- **Secure Design and Packaging Programs -** Concerns about hardware security threats and vulnerabilities have presented an opportunity for the Department of Defense (DoD) to reduce barriers by utilizing mainstream electronics technology while protecting critical defense technologies and manufacturing. As a result, the DoD has reevaluated trusted and assured access to advanced node foundry production over the last several years. The goal is to incorporate commercial industry ASIC and SoC (including SiP) capabilities while maintaining the integrity and security of defense systems [16]. Furthermore, in order to achieve more rapid modernization while reducing the size and increasing the performance of DoD systems, the department has launched various trusted and assured microelectronics programs as follows:

    1) **SHIP Prototype Project -** This program is sponsored by the Office of the Under Secretary of Defense for Research and Engineering and funded by the Trusted and Assured Microelectronics program. They established the State of the Art (SOTA) Heterogeneous Integrated Packaging (SHIP) program to create a sustainable industry and functioning standard for addressing government needs in Microelectronics (ME) packaging. SHIP will use commercial industry expertise to design a novel standard for ensuring DoD access to secure advanced packaging and testing. The standard will provide the DoD, and the Defense Industrial Base (DIB) with continuous access to a catalog of proven IP and chiplets that can be used to design and build customized multichip modules using commercial off-the-shelf state-of-the-art devices [17].

       The program's second phase will create multichip package prototypes and speed up the advancement of interface standards, protocols, and security for heterogeneous systems. SHIP prototypes will combine special-purpose government chips with advanced commercial silicon products from Intel, such as FPGAs, ASICs, and CPUs. This combination of technologies opens new avenues for the US government's industry partners to develop and modernize mission-critical systems while leveraging Intel's US fabrication facility [18].

    2) **DAHI Program -** The Diverse Accessible Heterogeneous Integration (DAHI) program was established to create transistor-scale heterogeneous integration processes integrating cutting-edge compound semiconductor (CS) devices and other emerging materials and devices with high-density silicon CMOS technology. DAHI's ultimate goal was to create a manufacturable, accessible foundry technology for the monolithic heterogeneous co-integration of various devices and complex silicon-enabled architectures on a common substrate platform. This kind of integration would boost the capabilities of high-performance microsystems for the US military. This program sought to address the following critical technical issues: (a) development of heterogeneous integration processes, (b) establishment of high-yield manufacturing and foundries, and (c) circuit design and architecture innovation [19].

    3) **CHIPS Program -** The demand for faster, more compact, and cheaper electronic devices has pushed the semiconductor industry to integrate various circuit blocks such as digital, analog, and analog-mixed signal blocks into an SoC. This integration has been enabled by advanced CMOS technology but has also increased design and processing costs. IP reuse has emerged as a tool to reduce overall design costs associated with advanced SoCs, owing to aggressive digital CMOS scaling for high-volume products. However, due to factors such as high initial prototype costs and requirements for alternative material sets, the monolithic nature of cutting-edge SoCs is not always acceptable for DoD or other low-volume applications. The Common Heterogeneous Integration and Intellectual Property (IP) Reuse Strategies (CHIPS) program seeks to create a new paradigm in IP reuse to improve overall system flexibility and reduce design time for next-generation products. CHIPS envisions an ecosystem of discrete modular, reusable IP blocks that can be assembled into a system with existing and emerging integration technologies. Modularity and reusability of IP blocks will necessitate widespread adoption of electrical and physical interface standards by the CHIPS ecosystem community. As a result, the CHIPS program will create the design tools and integration standards needed to demonstrate modular IC designs that combine the best of DoD and commercial design and technology [20].

- **Heterogeneous Integration Roadmap for Electronics Applications -** The Heterogeneous Integration Roadmap spans the complete semiconductor and electronics technology ecosystem in detail. It functions as a knowledge-based blueprint for future electronic technology. The roadmap is market- and application-driven, beginning with six market segments: high-performance computing and data centers, IoT, 5G communications and beyond, smart mobile, automotive, wearable and health, and aerospace and defense.

  The demand for next-generation systems has increased significantly, owing to emerging trends driven by numerous applications such as smart devices (House, TV, mobile, automotive), data centers, high-speed wireless communication, and medical and health care devices. As a result, technologies are evolving rapidly. However, they face complexity in keeping pace with the increased demand. For example, the number of globally connected

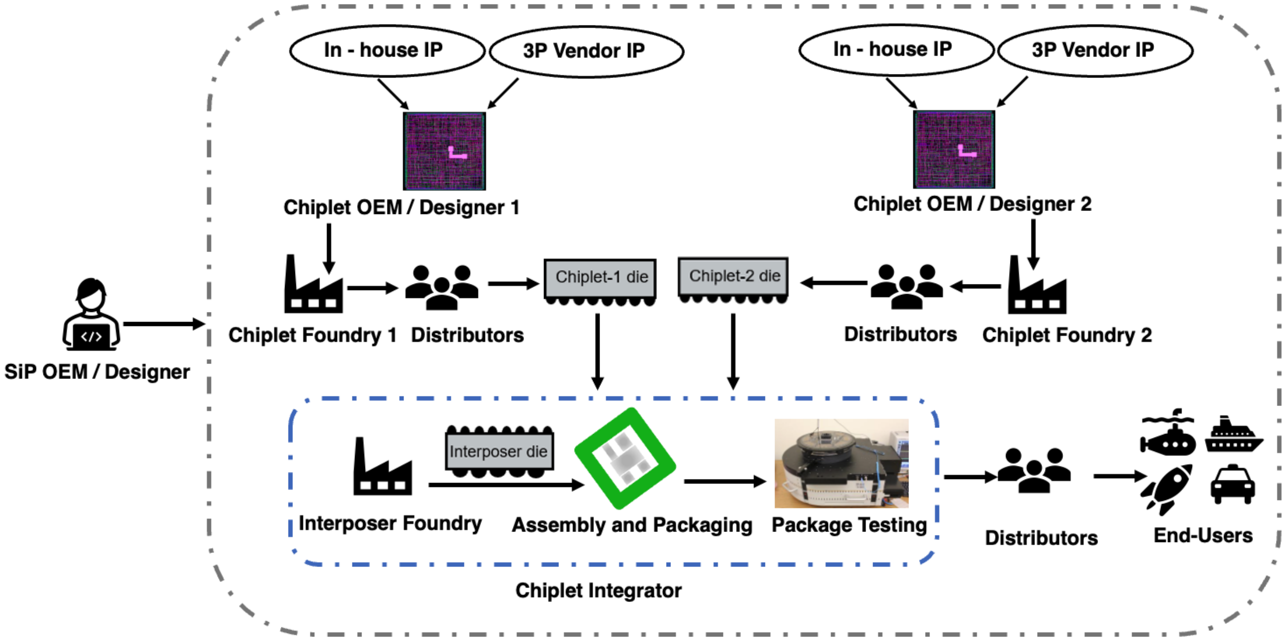


Figure 3: SiP supply chain for heterogeneous integration

IoT devices/endpoints reached 12.3 billion by 2021, and the projection is to be 27 billion by 2025 [21]. Manufacturing such a massive number of products requires a lower time-to-market and lower production costs, making the challenge surrounding conventional SoCs even more difficult.

Similarly, newer medical and healthcare products are primarily driven by miniaturization, implantability, and portability [22]. The recent trend towards various medical and healthcare equipment (e.g., pacemakers, neurostimulators, insulin pumps) focuses on smaller form factors and increased performance. In addition, modern medical wearables utilize different sensors to detect heart rate, blood pressure, oximetry, respiratory monitoring, hearing aid, and body temperature and incorporate IoT-based technology and cloud computing to provide better healthcare facilities.

Furthermore, there has been a momentous technological shift in the field of the automobile towards autonomous driving, and the industry emphasizes various security and safety features. Therefore, modern autonomous cars require high-performance embedded machine learning chips to collect and process thousands of images from various camera sensors embedded at numerous locations of the automobile. In addition, various safety and performance sensors (blind-spot detection, pedestrian detection, park assistance, collision detection, emergency braking system, cruise control, lane assistance) are installed, which require low power and high bandwidth data communication among internal components and processors, as well as intra/inter-vehicular communication [23].

To summarize the above discussion, next-generation electronic systems must ensure (1) high bandwidth, (2) low power, (3) smaller form factor, (4) increased functionality, and (5) flexibility [24]. Packaging different discrete IP blocks/components on a PCB may achieve the increased functionality requirement; however, the form factor is a large and less flexible design, requiring high chip-to-chip bandwidth, and the overall system power may increase. In addition, monolithic integration of the IP blocks inside an SoC design may solve some challenges with PCB; however, time-to-market is extensive and can incur IP maturity problems [24]. For example, a designer purchased an IP block from a vendor with a 40nm technology node, but the SoC is designed with a 14nm technology node. In this case, plug-n-play for the IP block is impossible as the design is less flexible, has increased time-to-market, and incurred a lower yield.

Heterogeneous integration of SIPs is the most appropriate solution to achieve the goal. It allows flexibility to choose known good dies from various vendors fabricated with different process nodes, integrates over active/passive interposer substrate, and allows higher bandwidth. For example, Intel used Stratix 10 FPGAs, and SoC utilized EMIB and AIB technology to integrate different IP blocks with shorter interconnects, thus creating lesser delay with support up to 58 Gbps of data [24]. In addition, the known good dies are available from various vendors and are easy to integrate, thus reducing time-to-market significantly. Although heterogeneous integration is more suitable for designing next-generation systems, it introduces newer attack surfaces that can be exploited to access various security assets. Therefore, appropriate security measures are needed to utilize the overall benefits provided by heterogeneous integration.

The roadmap to HI has opened an avenue for research and development to resolve HI design and security issues.

III. Chiplet Security: Risks, Threats, Vulnerabilities and Assurance

Chiplets are the main component of a system-in-package created through heterogeneous integration. Therefore, chiplet security is critical as a building component of the SiP because a system created with vulnerable chiplets can eventually result in a SiP package vulnerable to security attacks.

A. Threat Model for Chiplet Security

The chiplet design and fabrication process involves various entities such as a design house, third-party IP vendors, and a foundry. Like IC IDM, a chiplet OEM can do their chiplet design and fabrication, but a fabless chiplet design house relies on a pure-play foundry for fabrication. Therefore, chiplet security involves security from the design phase (RTL) to the SiP OEMs who procure chiplets for heterogeneous integration. So, ensuring the chiplet security will be a step towards the security of the SiP package. However, due to the severity and multitude of security threats associated with the untrusted pure-play foundries, we will primarily focus on the supply chain involving fabless design houses [25].

The fabless design house follows a horizontal business model in which fabrication, assembly, and testing of integrated circuits (ICs) are outsourced to offshore foundries and OSATs to reduce cost and time-to-market. Similarly, for chiplets, the fabless design houses are expected to follow the same business model (see Figure 4). The supply entities related to the chiplet security are presented in the threat model (see Figure 4). The SiP designer, also known as the original equipment manufacturer, is trusted because it is responsible for the security of SiP. A chiplet design house may use in-house and third-party IPs to develop a chiplet design. Then, it sends the design for fabrication to an offshore foundry. Depending on the geo-location or market reputation of a chiplet design house, it may be either trusted or untrusted. However, providing a chiplet IP to an offshore foundry can make the chiplet vulnerable to insertion of hardware Trojans or overproduction. Furthermore, a competitor design house can steal IP by reverse engineering, or a rival foundry can clone chiplets and sell them as authentic. Also, recycled chiplets can be a threat if carefully extracted from the SiP package by an untrusted distributor or an end user. Typically, recycled chiplets may not be perceived as a considerable threat due to the significant effort required to remove a chiplet from a SiP package. The chiplet attack vectors can impact the security of mission-critical applications, such as defense systems, airplanes, and health care, by causing early failure, data breaches, and reliability problems. So, in our threat model, the SiP designer/OEM is considered trusted. All other entities in the supply chain are considered untrusted. The design tools used during the generation of the chiplet IP are also considered trusted.

B. Hardware Attack Vectors

1) Hardware Trojans: A hardware Trojan is a malicious change in chiplets to sabotage the security of the SiP package or an electronic system in which the SiP package will be deployed. These Trojans can cause significant security concerns regarding the SiP's confidentiality, integrity, and availability (CIA- triad) [26]. For example, it can cause a denial of service to cause reliability issues, Man-in-the-middle attacks to get unauthorized access to confidential data such as encryption keys, and the bias of neural networks [26]. Hence these SiP packages cannot be trusted for critical government data-center and national security applications such as defense, space, and energy sectors [27]. In a SiP supply chain, a hardware Trojan can be inserted by either an adversarial IP designer or an untrusted foundry [28]. Based on the adversary, there can be different attack models based on the trust assumption with any of these entities [29]. Among them, the threat model of the untrusted foundry has been widely discussed in the hardware security community [29], [30].

2) Reverse Engineering: Concerns about reverse engineering (RE), a process of extracting an RTL level of design by deprocessing and imaging various device layers from fabricated integrated circuits, still exist with chiplets [31]–[33]. Competitor semiconductor design houses or adversarial foundries can perform RE to gain a competitive and financial edge. However, it can cause a revenue loss to the chiplet OEM, and the reverse-engineered chiplet may have reliability and trust issues. Furthermore, like chips, chiplet reverse engineering can be an extensive process requiring much effort and time, so an adversary may find SiP reverse engineering more beneficial than chiplet.

3) Counterfeit chiplets: A counterfeit chiplet can be defined as (a) an unlicensed chiplet, (b) does not meet the specification and performance of the OEM, (c) is not manufactured by the authorized contractors, (d) is a non-conforming, faulty, or used OEM product offered as ”new” (e) has inaccurate or erroneous markings, or documentation [34]. Counterfeit is a billion-dollar business and is easy money for the adversary. Nevertheless, on the other hand, the OEM faces revenue loss and tarnished brand reputation. For chiplets counterfeit chiplets can be classified in the following categories [35]:

- **Recycled -** Recycled chiplets like recycled ICs [36], [37] can be one of counterfeit types. Recycled ICs are a big industry; chiplets can be recycled like recycled chips. However, as chiplet recycling is at the silicon die level counterfeiting, the adversary must put more effort and use sophisticated methods for this purpose. The chiplets may be taken from a used SiP, repackaged, and then sold to the market as new. During this process, a chiplet may break or lose its functionality. A successfully recycled chiplet may perform poorly and cause reliability issues in the system-in-package. An adversary may find the recycling of SiP packages more motivating.
- **Remarked -** The counterfeiters remove the old marking on the die package of the chiplet and mark the package with a new identification number and generate forged documentation to sell it to the market as higher grade ICs [36]. In the remarking process, the chiplets old markings can be removed via chemical processes and new marks applied by the adversary. E.g., an adversary can remark a chiplet to change the grade of the chiplets, such as commercial-grade to military-grade chiplets.
- **Overproduced:** A offshore foundry can fabricate more chiplets than the number of chiplet a design house has ordered. These overproduced chiplets can enter the SiP

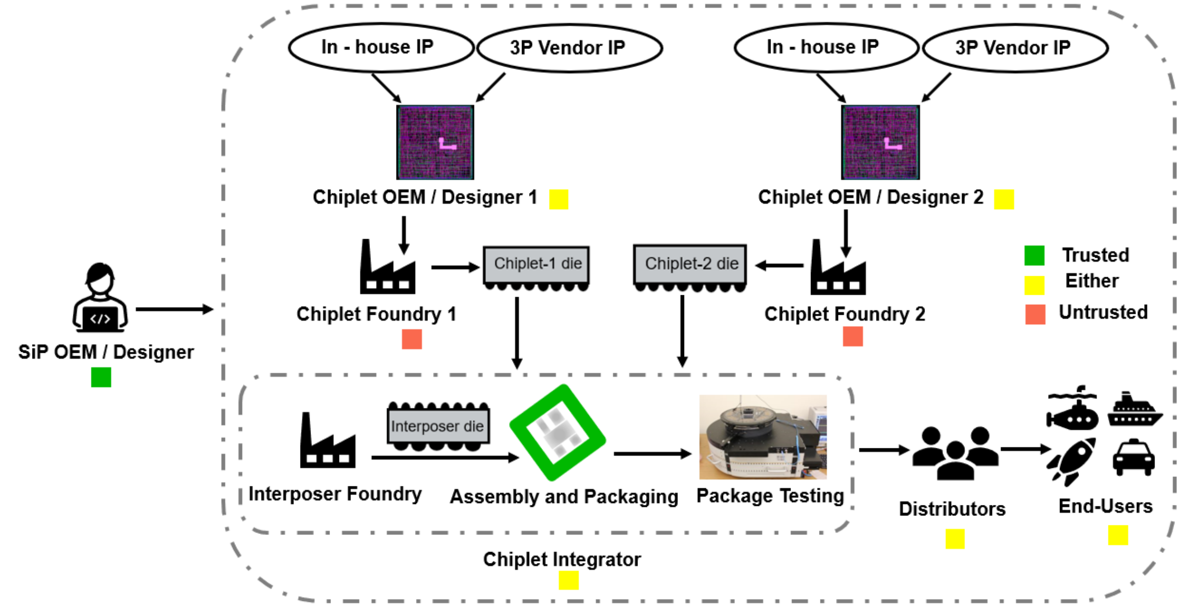


Figure 4: Threat Model of "Chiplet Security" for secure heterogeneous integration at different phases of the life-cycle.

supply chain through unauthorized channels [37].

- **Out-of-Specification -** After fabrication of chiplets, they are tested for the designed electrical parameters. A chiplet may still work, even if it fails to meet the design specification during post-silicon validation. However, it may be unreliable, slow, or vulnerable to security attacks. In addition, an adversarial distributor or reseller may try to sell these chiplets to a SiP designer as a high-quality chiplet. When the out-of-specification chiplets are integrated into the supply chain, it can be challenging to detect them during SiP system-level testing (SLT) [37], [38].
- **Cloned -** Chiplet can be cloned by adversarial foundries like competitors/counterfeiters to reduce the significant development costs of a component. A cloned chiplet is a replica of the original chiplet and sold as an authentic chiplet fabricated by or for the chiplet OEM [38].

C. *Trust Validation of Chiplets*

Trust validation of chiplets involves identifying tampering, counterfeiting, or malicious changes using various suitable electrical testing or physical inspection methods.

- **Testing - Logical Testing and Side Channel Analysis:** Logical Testing is a proposed method for hardware Trojan detection in SoC by using test vectors and observing a deviation in the output. It has its pros and cons, such as it is a non-destructive method, but it needs to trigger a Trojan to detect the presence of malicious change. For chiplets, a fabrication facility performs a wafer level testing, and it can be a challenge at the SiP designer end due to:
  - SiP designer needs to test every kind of chiplet, which requires time and monetary efforts.
  - SiP designer needs to acquire or develop a testing infrastructure for wafer-level testing of chiplet.
  - SiP designer needs test patterns from chiplet OEMs, which is subject to chiplet OEM's discretion.

  Side channel analysis can also be challenging due to the limited or absence of test infrastructure for chiplets at the SiP designer end, and besides this, it needs a golden model or signatures for trust validation, which is highly debatable when it comes to an untrusted foundry threat model.
- **Physical Inspection:** Physical inspection-based techniques typically capture nano-imaging (SEM-scanning electron microscopy) data from a polished thinned die [39]. There are two popular techniques, the first one, reverse engineering (RE), and the second *Trojan Scanner* [40] (see Figure 5 (A)). RE required SEM imaging data from all integrated circuit layers to reconstruct the netlist to compare with the original netlist. RE process is time-consuming, error-prone, requires highly skilled engineers, and many die samples are wasted during sample preparation. However, using *Trojan Scanner* [30], [41], [42], an SoC design house can perform trust validation of the die by using only active (or diffusion) layer SEM images and comparing them with a golden layout (trusted layout) to detect any malicious change. Therefore, it requires lesser time and fewer samples as compared to RE. In the SiP domain (see Figure 5 (B)), there can be multiple chiplet OEMs involved during the SiP design and development. RE can be a suitable method for counterfeit such as IP piracy detection, but it is a poor approach for Trojan detection due to the above-mentioned reasons. Chiplet trust validation using *Trojan Scanner* method can be challenging, and it cannot be directly applied for chiplets due to the following reasons:

1) It can be challenging for a chiplet OEM to entertain multiple requests from several SiP designers.
2) A chiplet OEM cannot share its golden layout to SiP OEM for trust validation to protect IP confidentiality.
3) Moreover, in various scenarios, a chiplet OEM cannot be trusted by a SiP designer due to various reasons, including geo-location of the chiplet OEM and foundry, the duration of presence in the supply chain, and brand image.

Hence there is a "void" for an entity or service or a validation mechanism in the SiP ecosystem for trust validation of chiplets using a physical inspection approach. It needs further research to develop a framework for SiP designers to perform trust validation of chiplets.

D. Attack Mitigation or Countermeasures

Chiplets are hardened IP which means their logic circuit is hardwired. Therefore, it can prevent an SiP designer from deploying a security feature if the chiplet security is ignored during the chiplet design phase. For example, to protect an SiP from an optical probing attack, the chiplet must have a security mechanism to avert an unauthorized optical probing attempt. Hence for SiP attack mitigation, a chiplet designer needs to consider various security vulnerabilities during the design phase. Later on, when the chiplet is integrated into a system-in-package, the package already has the necessary sensors or security features, which can be used to detect and trigger a necessary response against the SiP level attacks.

- **Design Obfuscation -** Hardware obfuscation is done with the aim of hiding design details and implementation details against reverse engineering and using design as a black box against IP cloning [43]. The obfuscation can be done at pre-synthesis, post-synthesis, and physical layout levels. In pre-synthesis, IPs are encrypted with IEEEP1735 [44]. Post-synthesis hides the actual functionality of the circuit using structural modifications of the design. Finally, at the physical level, the connections between the cells are obfuscated, such as doping-based methods and dummy contact insertion, so that the adversary cannot understand the layout design to perform reverse engineering and, in some cases, insert malicious circuits such as hardware Trojans.
- **Side Channel Resistant Designs:** The chiplet circuit designers need to consider the threat of side-channel attacks in the chiplets storing encryption keys and confidential data. In order to design a side-channel attack-resistant chiplet running a cryptographic circuit or having confidential data, the circuit's power consumption needs to be made independent of the performed operation and processed data. Hiding and masking are two methods of designing side-channel resistant cryptographic circuits [45]. However, these countermeasures cost additional circuit area and degrade performance. Furthermore, recent research shows that these countermeasures can be further attacked. So, higher-order hiding and masking techniques are recommended for designing side-channel resistant integrated circuits [46]. Finally, chiplet designers need to consider the trade-off between the level of security and the chiplet's power, performance, and area.
- **Sensors for Temper Detection and Prevention** Like on-chip sensors are used for detecting probing attacks. Similarly, a chiplet sensor (a hardened or designed as programmable logic similar to FPGAs) can detect probing and prevent further tampering. An optically active layer with angular-dependent reflectivity on an IC's backside protects it from semi-invasive physical attacks and optical fault injection attacks. Light emitted from a transistor's drain is detected in another transistor's drain after reflecting on the active layer that ensures no backside tampering. In addition, this layer is opaque to IR illumination, thus preventing photon-induced fault injection. Moreover, any damage to this protection from backside tampering can be detected by IC electronics [47], [48]. Another advanced solution can be CMOS compatible structures called nanopyramids that can mitigate electro-optical probing (EOP) and electro-optical frequency mapping (EOFM) attacks by scrambling the light signal reflected by these structures. Furthermore, the Nanopyramid structure can be applied to designated chiplets that require protection against EOP and EOFM attacks [49].
- **Security Primitives:** Security primitives are secure circuits that can be physically embedded into chiplets for mitigation against supply chain threats such as cloning, recycling, or overproduction. For example, physical unclonable functions (PUF) can be used to fingerprint a chiplet for authentication purposes to detect cloning. In addition, a silicon odometer can detect recycled components.
- **IP Secure Zones and Trust Modules (CHSM): Tamper Resistant Design -** The main objective of the chiplet hardware security module (CHSM) is to detect any security threat (e.g., Trojan, physical tampering) and provide a countermeasure and attack mitigation against hardware security attacks on individual components (chiplets) or complete system-in-package. CHSM considers both the chiplet-level and system-level tampering scenarios to make a heterogeneous integration tamper-resistant. To prevent system-level tampering, monitoring the electrical parameters of the interconnecting and interfacing components of a SiP is controlled by the CHSM module. In addition, monitoring the output signals from the backside (FEOL) and front-side (BEOL) IC tampering is processed by the CHSM as well. When a tampering or malicious modification has been detected, CHSM can stop communication between chiplets by blocking the communication channel and altering the data in confidential information-carrying signal nets to prevent confidentiality, integrity, and availability violation. Furthermore, the aforementioned detection methods of tampering through non-invasive and semi-invasive fault injection attacks (e.g., clock glitch, voltage glitch, EM, laser) at the chiplet-level are incorporated in CHSM to take preventive security measures during the run-time of an SiP. The preventive approaches include:

  - Blocking secure communication between IPs in a chiplet.

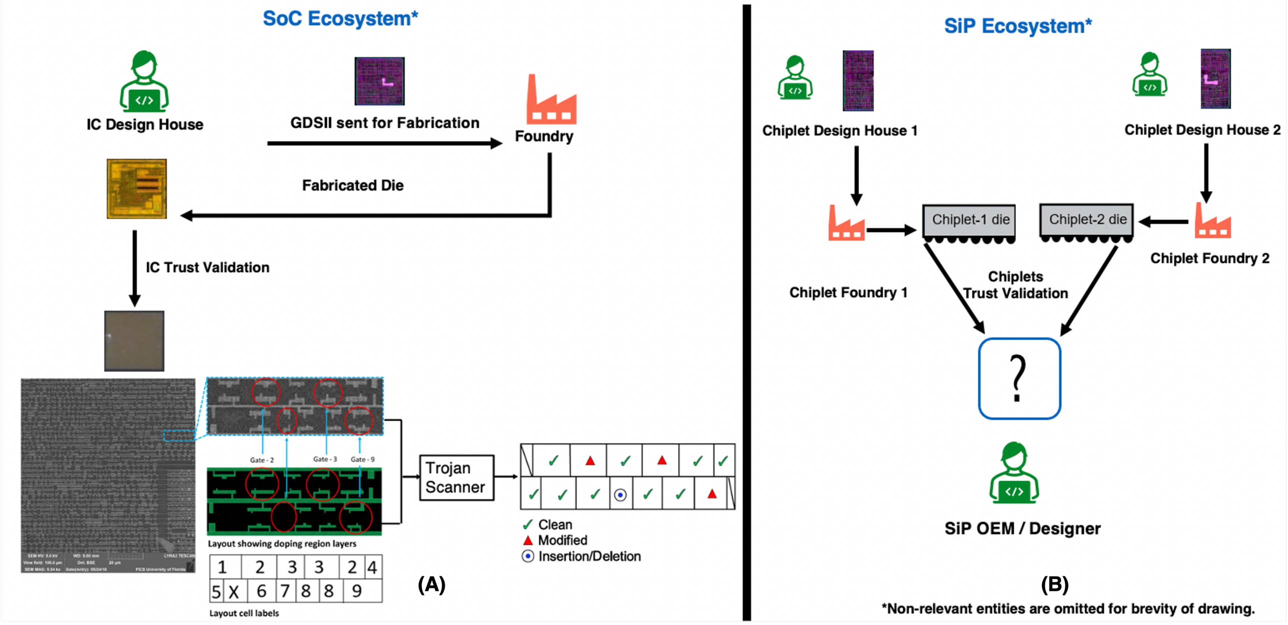


Figure 5: Trust Validation in SoC Vs. SiP Ecosystem.

  - Stopping the propagation of any malicious signal outside a chiplet.
  - Masking the injected faults.
  - Blocking the means of fault injection upon detection of the chiplet level tampering.

IV. Interposer and Substrate Security: Risks, Threats, Vulnerabilities and Assurance

The chiplet integrator uses redistribution layers (RDLs) to connect different components on a SiP. These components can be integrated using various advanced assembly methods such as build-up substrate, PoP (package-on-package), FOW/PLP (fan-out wafer/panel-level packaging), WLCSP (wafer-level chip-scale package), silicon interposer, Foveros, and EMIB (embedded multi-die interconnect bridge), etc. [50]. In the following discussion, interposer-based packaging technology will be used as an example to explain the vulnerabilities added to the existing system interconnect technology and the origin of the new assurance problems in heterogeneous integration.

A. Threat Model for Interposer Security

Let us look into the supply chain for heterogeneous integration after the chiplets are fabricated by the foundry (see Figure 6. There is an added complexity in the SiP design and manufacturing steps compared to the conventional SoC manufacturing process as chiplets need to be connected using advanced packaging technologies such as an interposer. A SiP designer procures the relevant chiplets for heterogeneous integration and sends the chiplets to a chiplet integrator. The chiplet integrator can perform multiple tasks based on their business model. While this integration process improves time-to-market and production cost, the added process steps and requirement for separate layers to establish interconnection can create a new dimension of threats such as Trojan insertion, SiP piracy, and reverse engineering. Furthermore, a chiplet integrator can play an adversarial role due to access to interposer design, chiplet types, and specifications. Hence it may or may not be trusted.

B. Hardware Attack Vectors

In the supply chain, the SiP designer creates the GDSII files for the interposer layer to be fabricated in the 'Interposer Foundry'. Once the interposer is fabricated, the interposer layer and the chiplets are sent to the assembly and packaging facilities, where all the components are integrated to create SiP. Unfortunately, the involvement of untrusted entities in the supply chain renders the heterogeneous integration vulnerable to attacks.

We consider three scenarios with combinations of trusted and untrusted entities in the supply chain to get a comprehensive attack surface for the interposer layer in heterogeneous integration.

- **Scenario-1:** The SiP OEM sends the interposer GDSII to an untrusted off-shore foundry to fabricate the interposer layer. Once the interposer is fabricated, it is returned to a trusted facility for assembly and packaging. An untrusted foundry may perform malicious modification/alterations to the GDSII of the interposer layer and change the parameters of the RDL or TSVs to cause reliability issues or incite leakage. For active interposers, the foundry may insert trojans [51] in the interposer layer. Because of the complexity of heterogeneous integration, these Trojans may be harder to detect during testing and verification. Furthermore, the foundry, having access to GDSII, has the potential to be complicit in IP piracy by giving away critical information about the interconnect network of the chiplet. The untrusted foundry can extract meaningful information from the interposer GDSII about interfaces and possible functionalities of chiplets based on the interconnect and TSV locations.

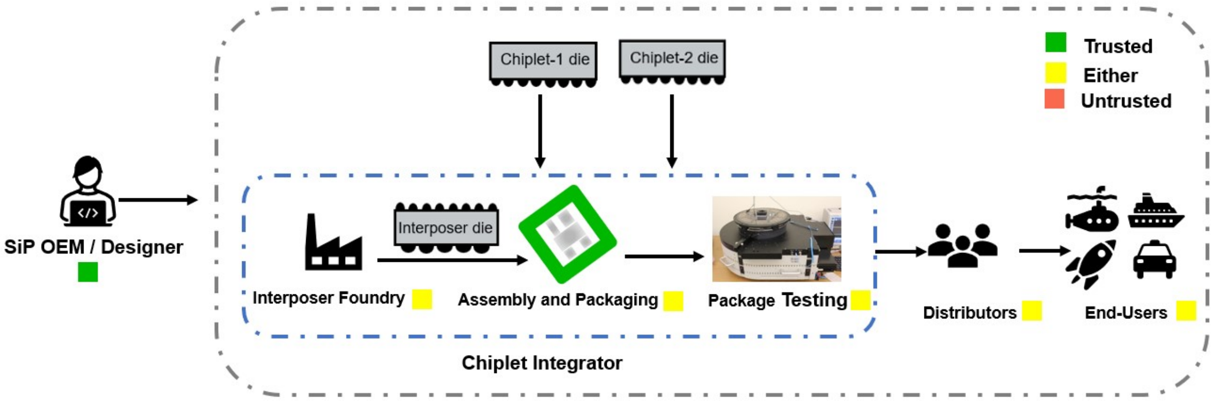


Figure 6: Threat Model for Interposer-level security

Table I: Attack Vectors concerning Advanced Packaging

Entity Scenario	SiP Designer	Chiplets	Interposer/ Si-Bridge Foundry	Assembly & Packaging	Package Testing	Distributors & End Users	Attack Vector
Scenario-1	Trusted	Trusted/Untrusted	Untrusted	Trusted	Trusted	Trusted	•Trojan Insertion •Reliability •IP Piracy
Scenario-2	Trusted	Trusted/Untrusted	Untrusted	Untrusted	Untrusted	Trusted	•Trojan Insertion •IP Theft •Overproduction
Scenario-3	Trusted	Trusted/ Untrusted	Trusted	Trusted	Trusted	Untrusted	•Reverse Engineering

- **Scenario-2:** The SiP OEM owner is a fabless design house that depends on off-shore facilities to realize the SiP design. In this case, the Interposer layer fabrication, along with assembly and packaging, is done in an off-shore untrusted environment like the service provided by many advanced packaging companies [52]. Therefore, the vulnerabilities discussed in Scenario-1 apply here. On top of that, since the integration is also done off-shore, adversaries in any part of these supply chain entities can better understand the whole SiP design. This scenario leaves the SiP vulnerable to stealthier Trojan-based attacks, counterfeiting such as overproduction, and IP piracy.
- **Scenario-3:** The whole SiP manufacturing process is done in a trusted environment, but the end-user (adversarial nature) or SiP distributor is untrusted. Because of the availability of high-resolution failure analysis tools such as X-rays, photon emission microscopy, and SEM, the packaged SiP remains susceptible to hardware attacks such as reverse engineering [33]. An adversary with little to no involvement in the manufacturing process can easily reveal the interconnections between the dies by reverse-engineering the integrating interposer layer. The separate interposer layer makes it easier than the monolithic SoCs to trace all the active and passive components integrated into the interposer. As the chiplets on a SiP become readily available in the market, adversaries may reverse engineer the SiP and fabricate their interposer layer to produce cloned SiPs.

All three scenarios are summarized in Table I.

C. Trust Validation by Substrate Verification

As mentioned earlier, the present microelectronics assurance techniques in the advanced packaging industry are focused only on reliability. Security assurance can barely be achieved with in-comprehensive tests that check for defects, reliability, and durability in specific conditions. As the fabricated active interposer layer goes through a similar manufacturing process as chiplets, many of the security threats and assurance techniques already discussed for chiplets can also be extended to the interposing silicon layer. The material and structure of the interposer layer can be inspected to establish trust and assurance in the post-fabrication or post-assembly stage in the horizontal supply chain. While both destructive and non-destructive detection techniques discussed earlier can be used to evaluate the interposer layer's integrity during in-process testing and failure analysis, the effectiveness may vary depending on the technology node and structural complexity of the interposer layer [53].

D. Attack Mitigation or Countermeasures

Rigorous testing and physical inspection of the structural integrity can effectively detect malicious modification or alteration of the interposer layer in an untrusted foundry. However, this comes at the cost of time. This method becomes even more difficult for scenario 2, where the system-level integration is outsourced. A possible way to circumvent this is to adopt innovative design-based solutions as a countermeasure. An active interposer-based root of trust was proposed by [54] to monitor data transactions between processor and memory modules. This active monitoring can be leveraged to detect malicious events between concerned chiplets. A sensor module may be devised to check for anomalies in run-time power consumption, electromagnetic radiation, and temperature that may serve as a trigger signal. Nevertheless, the integrity of these active schemes may become compromised if they are fabricated or assembled in an untrusted environment. Another way to ensure the integrity of this security module is to use reconfigurable FPGA. The FPGA can be embedded inside the interposer layer as an embedded FPGA (eFPGA) [55] or in the case of passive interposer-based SiP as a separate die which will serve as the root-of-trust. Even if the SiP is fabricated in an untrusted environment, the FPGA can be configured in a trusted facility. This FPGA-based solution can be devised to create a key-based permutation block [56] to obfuscate the design/ interconnection of interposed dies, making it harder to perform reverse engineering attack on the interposer layer. Furthermore, different layout-based obfuscation techniques in conjunction with logic locking to lock the dies or the interposer layer can be adopted to prevent IP piracy and SiP overproduction threats discussed in the next section.

V. SiP Security: Risks, Threats, Vulnerabilities and Assurance

Even if an individual chiplet and interposer go through trust validation and assurance checks, the final system-in-package (SiP) can also face similar security threats as an SoC from an adversarial end-user. These security attacks can exploit unidentified chiplet, interposer, and system-level vulnerabilities; hence, a SiP package can still be vulnerable to further attacks. This section discusses the security threats faced by SiP and their possible countermeasures.

A. Threat Model for Heterogeneous Integration for SiP

A SiP package is vulnerable to attacks by an adversarial user to compromise its security, intellectual property, and counterfeiting purposes (such as recycling or cloning). The risks associated with untrusted chiplet and untrusted foundry have been discussed in the previous sections. After procuring chiplets and interposer fabrication, they are sent to the chiplet integrator for heterogeneous integration. After packaging and testing, the SiP package is available through various channels (direct selling or distributors). Figure 7 shows the security risks involved at the package level, and the following sub-section discusses various attack vectors in detail.

B. Hardware Attack Vectors and Surface

Even a SiP package is securely assembled using trusted chiplets and interposer. However, the SiP package can be vulnerable to further attacks for various reasons. First, in some scenarios, it is not possible to perform trust validation, or the only option is to use a potentially untrusted supply chiplet to build a SiP [57]. Another reason can be an unknown vulnerability at the chiplet or interposer level. Possible attacks by malicious chiplets can be described as snooping on data intended for other chiplets, modifying data transferred between other chiplets, or an untrusted chiplet masquerading as a trusted chiplet. Also, in a heterogeneous SiP, individual chiplets are physically placed significantly closer than a PCB. Therefore, it increases the communication bandwidth and vulnerability to side-channel attacks by a malicious chiplet or an adversarial end user. Furthermore, various SiP level attack vectors are as follows:

- **Supply Chain Problems (Counterfeiting) -** The supply chain for heterogeneously integrated (HI) chips, like for monolithic chips, can experience threats of counterfeiting at chiplets and the package level. However, due to the structure and the involvement of multiple entities in the supply chain of HI chips, the threat of a chiplet integrator overproducing the entire SiP is unlikely, as the Assembly and Packaging entity needs to procure extra chiplets for the overproduction of the entire SiP. Moreover, that mal- practice will fall under cloning. In addition, other package-level threats from the SoC supply chain still exist in the HI supply chain, such as recycling, remarking, and out-of-specification. These counterfeiting problems can occur post assembly and packaging in the supply chain and follow a similar threat model to the SoC domain [25]. There may be potential threats in the HI supply chain which are not found in the SoC domain because of the introduction of chiplets. For example, a SiP package may be integrated with low-grade chiplets instead of the higher grade, which can affect the overall grade of a SiP package. Hence it can impact the SiP package's functionality and reliability. For example, a chiplet distributor may sell commercial grade chiplets to the SiP designer who expects military grade chiplets. Although this can be seen as a threat at the chiplet level, it affects the authenticity of the entire SiP package chip, which is intended to be military grade.
- **Side-Channel Attacks** - In HI, chiplets are placed in much closer physical proximity than an IC on a PCB board. It is especially true for 2.5D, 3D, and 5.5D designs. Unfortunately, this placement strategy increases the ability of a malicious chip to perform various power, timing, and EM-based side-channel attacks. For example, a malicious chiplet introduced into the system-in-package improves the sensitivity and spatial resolution of collecting EM, thermal, and power signatures from the other chiplets immediately above-below and adjacent to it by orders of magnitude [58], [59].
- **Fault-Injection Attacks** - The adversaries can exploit several fault injection attacks to leak secret information from SiP like the conventional SoC [60]. Heterogeneous integration of chiplets creates multiple attack points inside the SiP package, such as memory, processor (registers, or functional logic area), the vertical interconnects (TSVs), and the logic circuit in the active interposer. Besides this, the communication bus between different chiplets, the distribution network of the clock, and power can be the possible surfaces of fault injection attacks. A fault can be injected into the system using laser illumination, EM radiation, clock, or voltage glitching, propagating to an observable node. In the fault analysis phase, an attacker may perform a differential or sensitivity analysis to steal the assets, such as the encryption key. Although the 3D die stacking technology and heterogeneous integration provide the defense against

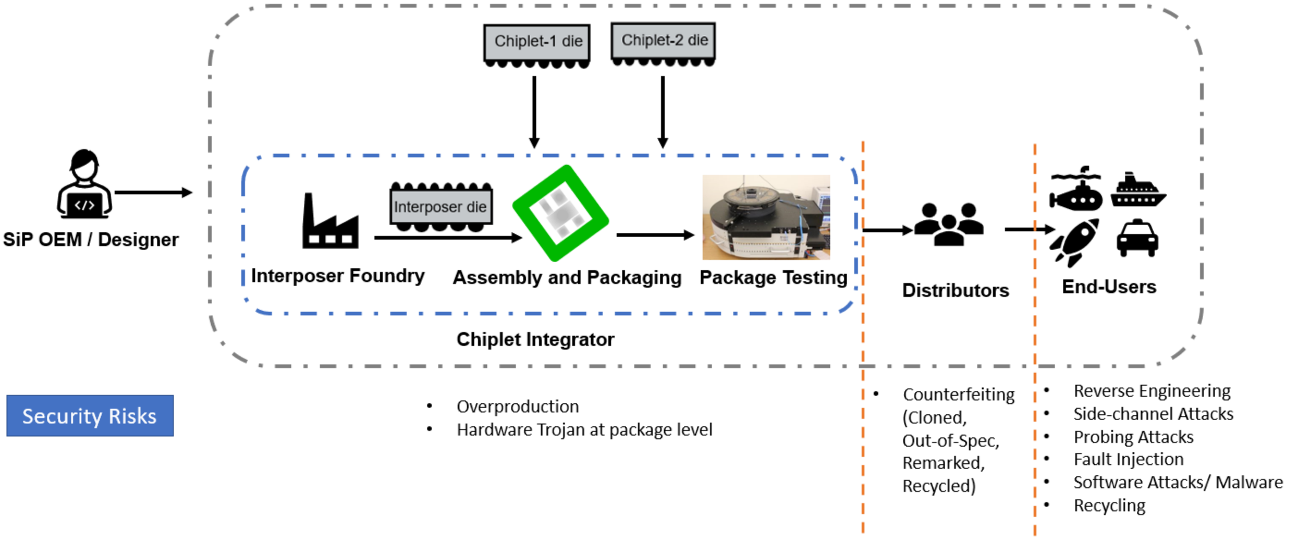


Figure 7: Threat Model for SiP Security

some fault injection attacks naturally [60], assessment of some attack surfaces is still required since design and integration complexity increases in a SiP. In addition, new attack surfaces have evolved beyond the traditional 2D packaging because the SiP package is built after integrating chiplets from various process nodes; their speed and supply voltage can be different. Furthermore, the fault injection techniques mentioned earlier make the SiP package vulnerable to timing attacks. In addition, the CAD tools for heterogeneous system design and verification may need a security assessment feature to perform security validation against the security threat posed by fault injection attacks.

- **Tampering -** The possibilities of tampering with a system in package (SiP) can be classified into two areas, chiplet-level tampering, and SIP-level tampering. Untrusted supply chain entities associated with a heterogeneous integration can be linked to these possibilities of tampering. For example, an adversarial IP owner or chiplet vendor can tamper with a chiplet during its design and manufacturing process (e.g., chiplet level tampering). On the other hand, tampering is also possible during the heterogeneous integration of SiP by a chiplet integrator (e.g., system-level tampering). In addition, an adversarial end user or black-hat attackers can tamper with physical attacks on chiplets or the integrating components of a heterogeneous system (e.g., vertical interconnects, communication interfaces, or interposer) by exploiting unidentified vulnerabilities. These tampering approaches may pose security threats and create hardware assurance issues that must be addressed during a heterogeneous system's design and integration step. The ways of tampering and their potential threats are briefly discussed as follows:

(1) Chiplet-level Tampering: There are various ways of SoC level tampering have been reported by black-hat (adversarial users), and white-hat (security researchers) attackers, which can be further extrapolated to chiplet [26]. The ultimate goal of chiplet level tampering is to leak confidential information (e.g., secret key or any asset). A chiplet can be maliciously modified during design time to insert hardware Trojans which facilitates confidentiality, integrity, and availability violations. An adversary can also perform a non-invasive attack without any physical alteration of a target device, and a semi-invasive attack requires a slight hardware change. For example, photon-induced current and EM radiations can be exploited to inject faults by flipping the bits of a memory chiplet, retrieving the stored bitstream of an FPGA chiplet, or registers of a chiplet having crypto hardware (e.g., AES, RSA, or SHA). A clock port, clock network, and power distribution network can tamper with advanced probing techniques (e.g., electro-optical, nano-probing) to assist clock glitching or voltage glitching attacks. Moreover, semi-invasive techniques such as focused-ion beam (FIB) help an attacker edit circuits to bypass security features or reroute a net carrying asset to attack the security of the system [61]–[63]. Tampering with probing can also enable an adversary to modify or read a signal directly inside the logic circuit of a chiplet.

(2) System-level Tampering: The main objective of system-level tampering is to alter the interaction between various functional chiplets, attack inter-chiplet communication, and reduce the strength of system-level security incorporated in heterogeneous integration. Malicious modification can degrade the reliability and signal integrity of the vertical interconnects that transfer signal and power from one chiplet to another. The change of design parameters of TSVs (through silicon vias) may affect reliable performance during run time and cause failure in operation [64]. During the design and fabrication of interconnects, a hardware Trojan Trojan (e.g., modification of logic in active interposer or silicon bridges of passive interposer) can be inserted in the interposer to bypass any security feature or perform DoS (Denial of Service) attack.

In the case of HI, a monolithic SoC is partitioned into different chiplets based on their functionalities. As a result, many communications within a single die now happen as inter-die communication. Generally, probing inter-chiplet interconnects is easier than probing a bus buried in a die between metal layers. Therefore, these interconnect between chiplet make the SiP vulnerable to probing attacks. Advanced probing techniques leverage the direct access to the interconnects and interfaces to circumvent the security module (e.g., remove and change connections between chiplets) and intercept secure communication among chiplets (e.g., modification or read-out of any signal nets).

- **Malware and Ransomware Attacks -**Malware is malicious software code that can harm an electronic system by leaking, destroying data, or in extreme cases, causing a denial of service (DoS) attack [65]. The government, non-profit agencies, and private companies worldwide have been attacked by malware and cyber-attacks, which cost them billions of dollars [66], [67]. Malware and ransomware must be handled at the SiP level since electronic systems use SiPs assembled through heterogeneous integration. An electronic system cannot be considered secure until all its parts are secure. To have a safe system, any system that employs SiP, such as an IoT, high-performance computing, or cloud server, must perform the security assurance of the SiPs used in that system. The system-level operation of the devices eventually comes down to hardware, and malware detection in hardware is very challenging unless the designers of the hardware/ chiplet integrators are aware of such attacks. So, by adding proper detection methods to the SiP package, malware and ransomware can be prevented to a great extent. Such methods are discussed in section V-D.

C. Trust Validation by System Verification

Heterogeneous Integration (HI) delivers flexibility advantages over monolithic SoC development due to its ability to integrate separately manufactured components into a higher-level assembly (SiP). However, since chiplets can be sourced from various supply chain entities, Die-to-Die communication can be vulnerable and lead to multiple attack vectors and surfaces. Further, a SiP package can be a counterfeit one that can cause reliability issues in the end-user applications and a significant revenue loss to the SiP designer. Package level potential attacks and vulnerabilities can be detected and avoided by enforcing security policies to monitor the transaction between chiplets. Additionally, an end user can use provenance-based methods to verify the authenticity of a chiplet.

- **Security Policies -** In the context of security verification, security policies specify the confidentiality, integrity, and availability requirements for specific security-critical assets and provide mitigation strategies that need to be implemented [68]. For example, an encryption module can only respond to encryption requests by other IPs and take encryption keys as input if the system is not in debug mode. Otherwise, an untrusted debugger can violate confidentiality and integrity requirements. Therefore, a security policy can be enforced which monitors the debug signal and deny all encryption requests when a debug request is accepted by raising a flag. This policy ensures that a secured communication standard between the encryption module and other IPs can be established. Similarly, a set of security policies can be derived from the design specification for secured communication between chiplets in HI. A chiplet-based hardware security module (CHSM) can be utilized to enforce these policies during chip operation. The security policies can be placed in the form of sensors or monitors in the silicon to operate in the run-time, and the CHSM can raise a flag if any violation of the security policy is detected during the communication between chiplets. Hence, a policy-driven post-silicon security verification methodology can be established for secured communication between chiplets. We will discuss more security policies in section V-E.
- **Provenance Detection -** With the globalization of the semiconductor industry, the supply chain entities are spread across the globe. Due to these outsourcing practices of fabrication, assembly, and packaging, many package-level threats can impact SiPs, such as counterfeiting. In the SoC domain, counterfeiting includes recycled, cloned, remarked, or overproduction of SiPs. These nefarious and lucrative threats can create devastating threats to mission control applications such as space, military, energy, and healthcare which may be using chiplets integrated on a SiP. Various strides have been taken to identify these threats in the supply chain, and methods are created to prevent and detect some or all of these counterfeit scenarios. However, in reality, methods rarely protect or prevent all threats but are specialized in preventing a few. For example, a framework called Secure Split-Test (SST) was introduced in 2013 to instantiate a more robust and secure interface between the IP owner and foundry/assembly facilities by mandating specific interactions between these entities like sending keys and validating results [69]. Furthermore, on-chip security primitives such as physically unclonable functions (PUF) and silicon odometer readings can detect cloned ICs [70]. However, these methods cannot verify all previously mentioned counterfeit instances. Furthermore, not everyone in the supply chain is familiar with the technology for performing these time-consuming verification processes.
  Another recent innovative strategy proposed involves incorporating provenance methods using a blockchain framework called *eChain* to create an ecosystem of trusted microelectronics to thwart the recycled, cloned, remarked, and overproduced ICs [25], [71]. Blockchain technology, introduced by Satoshi Nakamoto in 2008, provides a framework for a distributed database with an increasing ledger of blocks ensuring decentralization and consensus by all nodes as to the validity of a transaction [72]. The *eChain* framework is similar to that of the Bitcoin blockchain network, with changes (such as a consortium of already vetted members) geared explicitly toward ensuring electronics supply chain integrity.
- **Limited testability -** Heterogeneous Integration introduces new challenges for chiplet and complete SiP

package testability. For example, in the case of 3D ICs, one can access DFT pins only through the base die. Currently, many types of interface protocols and packaging technology exist for chiplets. However, there is no interoperable testing and debug standard for HI. Furthermore, because chiplets can come from a diverse supply chain, the lack of standard testing infrastructure creates a challenge for effectively testing the final SiP. Additionally, a testing infrastructure can pose a major security risk if proper design-for-test or design-for-debug algorithms are not used. For example, scan chains are frequently utilized as one of the most effective attack surfaces. To provide a standard test infrastructure, IEEE has proposed IEEE 1838 standard [73] for 3D IC testing. This standard can also be applied to 2.5D ICs. Also, IEEE EPS has published the best-known methods for HI testability which manufacturers and designers can use to ensure proper testing of a HI product [74].

D. Attack Mitigation or Possible Countermeasures

As discussed earlier, a SiP package can face in-field threats by an adversarial end-user. Therefore, the SiP level vulnerabilities need to be addressed by deploying relevant countermeasures against a particular attack as follows:

- **Fault Injection Detection:** Different types of fault injection techniques, including fault injection through clock glitch, voltage glitch, laser illumination, and EM radiation, can impact the timing delay in the victim device. A TDC (Time-to-digital converter) sensor capable of sensing the fluctuation in the delays of several components (logic gates, interconnects) of a heterogeneous system can be used to monitor fault injector attempts. This kind of sensor is proposed as FTC (Fault-to-time converter) sensor and demonstrates success in detecting attempts of different fault injections [75].
- **Timing Fault injection Mitigation:** A heterogeneous system has a set of security policies that define the security of the secret information of the system. An adversary can leak assets or reduce the strength of the security of the system by injecting controlled timing faults at the security-critical locations and ultimately by violating the defined security properties. Pre-silicon analysis paired with modifying the physical design parameters (e.g., gate size, interconnect length and width, power pads) can tune the delay of the security-critical paths and make the delay distribution uniform. These modifications will ultimately make a controlled timing fault injection uncontrollable and hide the impact of controlled faults. In summary, a preliminary security property-driven assessment with a set of physical design rules can reduce a design's susceptibility to timing fault injection attacks [76].
- **On-chip Cryptography:** It can ensure the CIA triad for messages, signals, and confidential information exchanged between chiplets. For example, hash-based message authentication code techniques can be used to send-receive signals between two chiplets which requires message integrity. In addition, the authenticated encryption protocol can be used if the signals require both confidentiality and integrity.
- **3D Trojan Detection and Mitigation:** The complementary characteristics of DCVSL (Differential Cascade Voltage Switch Logic) can detect malicious modification (parametric hardware Trojans on TSV) or external voltage glitches. Any tampering or malicious modification on the power or ground lines prevents the output of a DCVSL from being complementary, thus asserting a warning signal [64].
- **Clock Tampering Detection:** A buffer-based delay chain can detect a clock glitch or tampering. The upper boundary of the clock frequency is predefined by the propagation delay (T_d) of the delay chain. Timing violations may occur if the tampered or glitched clock runs faster than the upper bound ($1/T_d$). Therefore, the upper bound is set to equal to the critical path delay to ensure the best performance. The comparison result of the delay chain detects the possible glitch injection or clock tampering [77].
- **Sensors and Protective Shields :** Active internal shielding techniques can be exploited to prevent front-side probing attacks in a heterogeneous system [62]. These shields can be integrated into the SiP after the assembly and testing. An active protection technique can detect system-level tampering that senses any change in electrical parameters (e.g., resistance, capacitance, or inductance) of a heterogeneous system due to tampering [78]. Anti-tampering sensors such as light, pressure, and electrostatic or electromagnetic sensors can be integrated into the chiplets to notify the security controller unit whether the SiP has physically tampered or attacked. The security module can also periodically monitor the resistance of different components (e.g., TSVs, horizontal traces through the interposer, interfaces, I/O pads) that compares the measured values with pre-stored initial values and gives a decision on whether tampering is performed or not. One of the challenges with these approaches is that the chiplet is a hardened IP with almost nil scope for modification. In this scenario, a chiplet designer has to incorporate these security sensors during design to ensure they are fabricated on the chiplet, or a chiplet designer leaves some programmable logic space similar to FPGA. Then, SiP design security engineers can configure this programmable logic to design a circuit that can work as a sensor.
- **Side Channel Attack Mitigation:** This section will focus on 2.5 D HI packages because 3D packaging provides various attack mitigation due to its inherent stacking architecture that creates a natural countermeasure against fault and cache-based timing side-channel attacks [60]. At the 2.5 D SiP level, side-channel attack simulations can assist security researchers in uncovering system-level vulnerabilities. Commercial CAD tools provide fast and efficient transistor-level simulations for EM and power side channels. However, to make a system resilient against EM, thermal, timing, and power side-channel attacks, it needs countermeasures at different levels, such as low-leakage transistors, randomized operation at the system level, and side-channel attack resistant algorithms.
- **Malware and Ransomware Detection:** Malware and ransomware can frequently mutate (employ polymor-

phism) to evade signature-based detection techniques such as anti-viruses. Therefore, advanced detection schemes based on hardware performance counters and machine learning have been proposed in the literature to identify zero-day exploits by classifying microarchitectural hardware events associated with the program's execution [79]–[81]. Another way to detect malware is by putting power sensors [82] within the SiPs where a power side channel-based disassembler [83], [84] can be utilized in real-time to detect malware. Despite the space overhead caused by the addition of power monitoring sensors, the approach can still be used depending on how crucial the application is. Another possibility is to use machine learning techniques to improve the systems' ability to detect malware [85], [86].

- **On-Chip Security Module:** Like SoC, a SiP level security controller can monitor chiplet and their interfaces for any potential security property violation, run-time detection of hardware trojans, and tampering. Furthermore, it can use a machine learning-based approach to detect new Trojans. Its firmware can be updated to provide the controller with new Trojan signatures and updated security policies. A chiplet hardware security module (CHSM) can be one of the futuristic approaches as a security controller that be implemented on SiP package, which can co-ordinate possibly with chiplets to detect and neuter above mention threats. Concept and working of CHSM is discussed in details in section VI-C.

E. Security Policies

Security policies refer to a set of rules or requirements to protect the assets and IPs. For example, security policies are widely used in an SoC device to prevent unauthorized access, or transaction inside the device [87]. Furthermore, for secure heterogeneous integration of chiplets, security policies can help designers to develop design constraints and forbidden user actions to prevent any CIA triad violation.

There are two types of assets, primary and secondary. Primary assets may include the cryptographic keys and configuration registers which are the main target of attackers. Secondary assets mean the infrastructures that require protection to ensure the security of the primary assets. Security policies can enforce the confidentiality, integrity, and availability requirements of SiP packages on the system level as follows:

- **Confidentiality:** Only authorized entities will have access to an asset. Temporal validation will be required for those permitted entities. For example, Chiplet A may only receive hash data from the crypto core if it is the entity that sent out the data to be hashed in the first place. It will not be able to obtain hash output from the crypto core at any other time.
- **Integrity:** An asset cannot be modified by an unauthorized entity. For example, an unauthorized transaction (by a user, chiplet, or firmware) cannot change the data transferred from chiplet A to chiplet B while it is in transit.
- **Availability:** An authorized entity should be able to reliably access an asset when needed. For example, if a logic-locked entity requires an unlocking key to function, this key should be available to it whenever required.

Based on these requirements, many security policies can be formulated. Below, we enlist some of the standard policies. Of course, this list is not exhaustive but can provide a good understanding of various policies that can be implemented.

1) Access Control Policies: Access control policies specify how one chiplet can access an asset during different execution points for the SiP. These are:

- An unauthorized chiplet cannot access memory in the protected address range.
- An unauthorized chiplet cannot write out data to a restricted memory region (information leakage).

2) Information Flow Policies: Information Flow Policies restrict leakage or modification of information related to secure assets. Examples of such policies are:

- An unauthorized chiplet cannot access data intended for other chiplets during transit.
- An unauthorized chiplet cannot modify data intended for other chiplets.
- Chiplet A cannot pose as chiplet B to receive data intended for chiplet B.
- Data intended for a chiplet cannot be blocked by an unauthorized chiplet.

3) Liveness Policies: Liveness policies ensure that SiP can execute normal tasks without interruption. Examples include:

- A chiplet cannot flood communication fabric with messages to disrupt normal behavior (DDoS).
- During operation, the number of messages sent by an untrusted chiplet should not exceed the threshold of the maximum limit.
- The limit on the number of packets generated by an untrusted chiplet can only be assigned and updated at secure boot time.

4) Active Monitoring Policies: Active monitoring policies ensure the secure operation of the system during runtime. Examples of such policies are given below:

- The frequency of the clock signal cannot vary out of range to prevent the clock glitching.
- The voltage supplied to individual dies cannot vary out of range to prevent power glitching.

5) Security Policy Enforcement: CHSM is responsible for enforcing security policies. For this purpose, the high-level policies mentioned earlier need to be converted to formal constraints [88]. First, the assets in the system that need to be protected should be listed. Then, security policies involving that asset will be identified. These security policies may need to be modified or expanded while moving from one abstraction layer to another [89]. After that, possible attack surfaces will be identified, and necessary protections can be developed. Finally, these policies can be implemented in CHSM firmware, using a secure boot mechanism so that an adversary cannot modify the policies. Also, if the authorized owner needs to update the security policies, he/she can do it by upgrading the firmware.

VI. Roadmap Towards Future Research

In previous sections, based on our previous research and development in the SoC domain, we have drawn parallelism between SoC and SiP level threats and vulnerabilities and their respective probable trust validation attack mitigation. However, these SoC-level pre-existing solutions need further research and development (including enhancement and modification) before a security researcher can directly import these solutions for chiplet or interposer level security and, ultimately, secure heterogeneous integration of SiPs. Here are the following a few areas that open up a roadmap for future research work in the area of secure heterogeneous integration:

A. Trust Validation of Chiplets for Chiplet Security

As discussed earlier in section III-C about a strong requirement for trust validation of chiplets in SiP ecosystem. In the future, a better trust validation approach will be available on demand. This approach will not require a chiplet OEM to share its IP for trust validation of chiplets, and still, it can bring trust between chiplet OEMs and SiP OEMs. One possible approach could be an independent entity that can handle trust validation requests from SiP OEMs and perform trust validation on behalf of chiplet OEMs to provide validation results in a couple of hours to a day. This independent entity can work like *Interactive proof system*, in which a *prover* has access to computational resources, and *verifier* has limited computation power but seeks an answer to the problem, which is here trust validation. This independent entity can certify a chiplet as authentic or flag it as malicious based on the validation outcome; henceforth, we call this entity by Certificate Authority (CA) [90]. The notion of CA is based on an incentivized approach over an enforcement approach, which encourages most chiplet OEMs to join this certification authority, as they can be benefited by becoming trusted chiplet OEMs in the supply chain, which can boost their revenue and brand reputation. Also, penalties can be imposed if malpractice is detected to keep a sanity check on chiplet OEMs.

The trust validation process can start with a voluntary enrollment of a chiplet OEM with the Certificate Authority (CA) by sharing the active region footprint of logic cells; henceforth, we call it as *Minimal Layout* (see Figure8). In this way, chiplet OEM can protect its IP by sharing not all but necessary information to the CA. After this, CA can develop an SEM imaging specification and a validation model. Once a SiP OEM approach CA for chiplet validation of chiplet(s), CA shares SEM imaging requirements and classifies the chiplet as malicious or authentic based on the outcome of the validation model developed earlier. Various steps of CA design & development and validation process are described through algorithm 1.

B. Secure Die-to-Die Interface for Interposer Security

Protecting the Die-to-Die (D2D) communication system in heterogeneously integrated systems is critical in preventing eavesdropping and the growing number of hardware hacking attacks. A hardware solution is required to ensure a secure chiplet-to-chiplet communication interface via advanced interface protocol. In order to meet adaptability, low-cost terms, and varying bus performance requirements, a scalable wrapper/interface IP-core must be designed and implemented. It enables the authentication of various bus participants and the encryption of chiplet-to-chiplet buses using a single primitive. The solution must be transparent and easy to configure in any D2D interface system for SiP chiplets that will support a diverse range of chiplets available in the market. In order to protect the bus system/D2D communication with a minimum hardware overhead while considering all possible interposer level threats, the security feature should be simply implementable into the standardized interface bridge.

Algorithm 1 Certification Authority (CA) for Trust Validation of Chiplets

```
procedure ENROLMENT
    Chiplet OEM joins CA
    Agrees to terms & conditions of CA
    Share Minimal Layout to CA
    SiP OEM sign up as verifier
procedure CA DESIGN AND DEVELOPMENT
    SEM imaging specifications
    Trust validation model
procedure TRUST VALIDATION PROCESS
    SiP OEM request for chiplet validation
    CA shares SEM imaging requirements
    SiP OEM shares chiplet's SEM images
    if Validation = No Change Detected then
        Chiplet Certified as Authentic
    else
        Chiplet Flagged as Malicious
```

C. Chiplet Hardware Security Module (CHSM) for Secure SiP

It is clear from the earlier discussions that the heterogeneous integration has instigated various vulnerabilities in the SIP from its multi-party supply chain and manufacturing flow which can cause various counterfeit, hardware assurance, and trust problems. As heterogeneous integration follows a different manufacturing flow compared to the SoC, existing solutions developed for typical SoC design may not be enough to solve the challenges mentioned above. For example, prior research proposed various trusted computing architectures to prevent attacks on SoCs. AEGIS [91] is one of the earliest secure architectures which protects memory tampering from possible software/hardware-based attacks. It protects the integrity of the software program by calculating the hash of the secure kernel at the initial boot.

Moreover, the secure kernel is responsible for ensuring AEGIS secure functionalities. Here, the processor is also trusted, and the on-chip cache is assumed secure against physical attacks. Furthermore, the trusted platform module (TPM) [92] also protects the software by measuring the integrity metric of the successive programs starting from root-of-trust for measurement (RTM) and stores the hash of programs inside the platform configuration register (PCR), thus creating a chain of trust. In addition, TPM uses endorsement keys (EK) unique to each chip serving as a master derivation key, attestation identity key (AIK) for creating digital signatures, and storage keys to protect the memory by storing encrypted programs and data. However, none of the above architectures are applicable in HI as the processor because memory, processor, and other

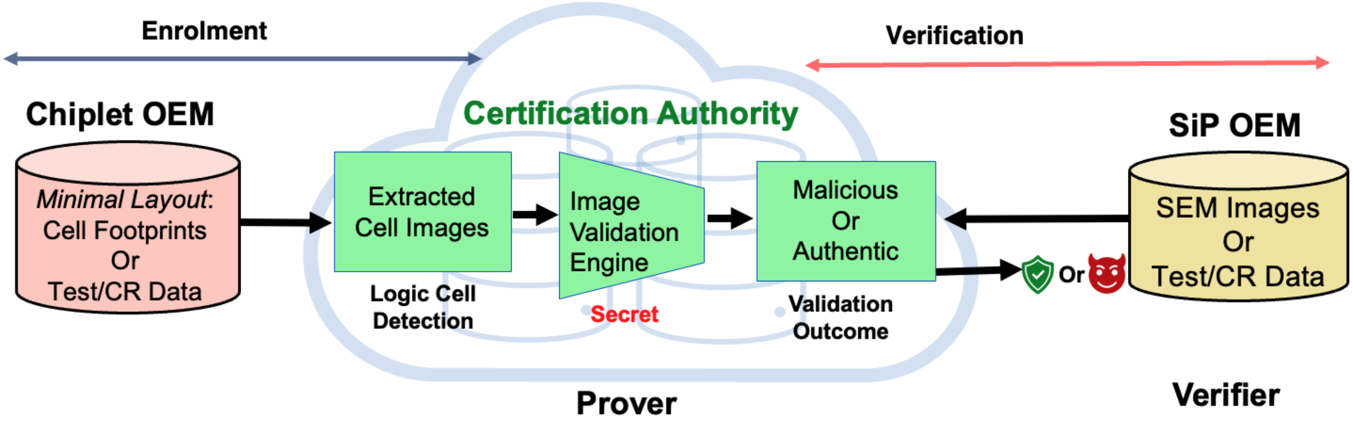


Figure 8: Certification Authority for Trust Validation of Chiplets.

components are integrated as separate chiplets and prone to attacks on the insecure communication channel.

In addition, the ARM TrustZone [93] is a well-known industry-developed architecture for ensuring SoC security. TrustZone protects the trusted hardware and software resources by isolating the Trusted Execution Environment (TEE) or the secure world and Rich Execution Environment (REE) or the normal world using a Non-Secure (NS) bit at the bus architecture. The hardware and software resources running in the normal world do not have access to the components in the secure world, although the opposite is allowed. Therefore, this hardware-based security solution is well suited for SoC as the communication within the secure world happens in plain text, which is prone to physical attacks in the heterogeneous integration. Similarly, Intel Software Guard Extensions (SGX) [94] create "enclaves" where the trusted execution of programs happens, and unauthorized access to the enclaves is not allowed. There are other security architectures (e.g., Bastion [95], Sancus [96], and TyTan [97]) which are developed to provide security for an SoC design, however, significant changes are needed in the designs considering the threat model of heterogeneous integration.

Therefore, one of the possible solutions for the challenges mentioned above is to design a centralized chiplet that will act as a hardware security module to prevent all possible attacks based on the HI threat model. We refer to the chiplet as CHSM, which is assumed to be trusted (see Figure 9). As stated earlier, the heterogeneous SIP designer has no control over many of the chiplets procured from third-party vendors and can not trust those chiplets. Thus, the trusted CHSM plays a vital role in ensuring the overall system's security. In [98], the authors proposed an end-to-end secure SoC lifecycle flow where the SoC contains a root-of-trust security engine (SE). Similarly, the heterogeneous SiP requires a secure manufacturing flow to make it free from all possible vulnerabilities mentioned earlier, and the CHSM acts as a root of trust. The CHSM contains various static security assets (e.g., a device-specific identity (ID), private keys, keys stored in effuse.) to perform various cryptographic operations and encrypted communication between CHSM and chiplets. Therefore, these security assets must be provisioned inside the CHSM securely on the manufacturing floor or in a trusted facility. POCA [99] provisions security assets securely inside the chip at the zero trust stage of the manufacturing floor. Thus, CHSM must integrate POCA infrastructure inside it to provide security assets securely on the manufacturing floor.

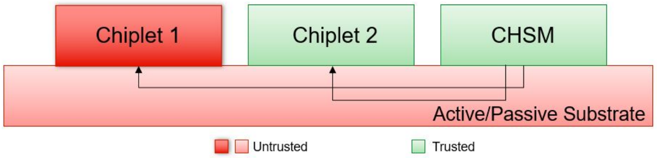


Figure 9: High level block diagram of CHSM inside SiP.

CHSM can be implemented in the embedded FPGA platform, which may contain a fully FSM-based hardware controller or a processor with firmware support. During in-field operation, the CHSM authenticates the chiplets and generates a shared secret key to encrypt the communication between the two chiplets. Encrypting every communication between chiplets can be hazardous in terms of performance. In addition, the system-in-package may not need all chiplets to be trusted and all encrypted communications. However, the channel must be encrypted between the CHSM and the chiplets when the chiplet contains security assets and runs any mission/security-critical applications. Thus, the performance and security of the SiP and security applications can be ensured efficiently. The CHSM monitors the data communication among chiplets to determine any malicious activity by Trojan implanted inside SiP package or malicious software. The CHSM contains security policies to detect the anomalies of the data communication or illegal access by untrusted software/hardware entities to the protected region. Once an anomaly is detected, the CHSM protects the security assets, prevents malicious activity based on the security policies, and creates a protected boundary where the malicious implant/software cannot access the trusted resources. The CHSM contains various sensors to detect physical attacks (e.g., laser, X-ray, voltage/clock glitching), and it protects the SIP based on the security policies. In a nutshell, CHSM acts as a root of trust inside the SIP and protects it from all possible vulnerabilities from the manufacturing floor to the end of life. Figure 10 shows the high-level block diagram of the CHSM IP and its components.

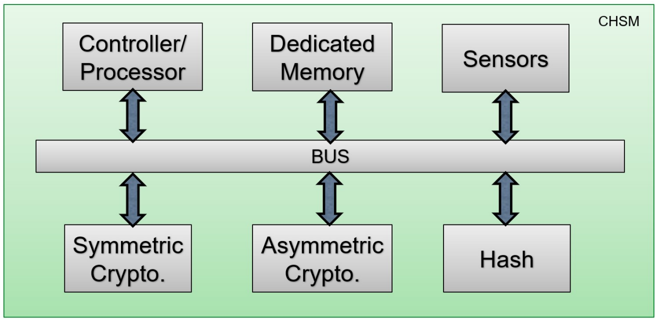


Figure 10: High level block diagram of CHSM IP.

1) Provenance Method to Identity Counterfeit SiP: For SiP hardware assurance, the complete package and its components must be traced back to its source of origin using provenance methods. Assuming all supply chain entities are known and vetted, it is very challenging for an adversary to inject a counterfeit SiP package into the supply chain. However, if an adversary successfully infiltrates a counterfeit SiP in the supply chain, that entity can be identified using provenance techniques such as blockchain [100].

The question arises: Can preventative measures like these align with the newer heterogeneous integration processes? Assuming a Chiplet Hardware Security Module (CHSM), introduced in the previous section, can be utilized in the HI, many pre-integration threats could be alleviated. However, this leaves provenance post-integration as a vital goal; once the HI chip is integrated and assembled, the authenticity of the chip needs to be asserted in the remaining phases of its lifespan: as an element assembled in a PCB, in the field, and at the end of its life.

- *SiP Manufacturing Phase:* This phase involved procuring individual chiplets, assembly on the interposer layer, and producing the final SiP package. Tracing and tracking individual components of a SiP can thwart counterfeit chiplets and further impede a counterfeit SiP package from the supply chain.
- *Assembly on PCB Phase:* As a PCB component, the integrated SiP performs its complete operations as one part in an extensive system of components. The component is assembled onto the PCB along with the other components by a PCB design and assembly house.
- *Field Deployment:* As the PCB is deployed to the field (typically inside a system) and operating at its intended application, the SiP is an active member functioning in the system.
- *End of Life:* Once a system is not in service or an individual component has been stripped from its PCB due to a failure or preventive maintenance. In this scenario, that system or component is no longer utilized in its intended functioning system, and it has reached the end of its life.

The goal of provenance methods is to verify the authenticity of heterogeneously integrated packages by tracking and tracing a package to its origin, recording ownership records, and its life events, such as the end of the life.

VII. Conclusion

The semiconductor industry is pacing toward heterogeneous integration with a broad focus on making heterogeneous integration as easy as "LEGO -Assembly." After discussing enough motivation for heterogeneous integration. This survey cum perspective paper on secure heterogeneous integration tries to bring the attention of chiplet and SiP designers, hardware security researchers, and SiP customers to the unforeseen security risks, threats, and vulnerabilities at every level of heterogeneous integration. First, the threat models were derived for every level, from procuring chiplets to interposer design and final chiplet integration. Next, the attack vectors and surfaces were identified for every stage, such as insertion of hardware Trojan, counterfeit chiplets/ SiP, and package level attacks to comprise the CIA triad. Then, trust validation methods were analyzed for the risks and threats identified earlier to the authenticity of chiplets and assurance. After that, attack mitigation was analyzed for possible in-field attacks such as side-channel, fault injection, probing, and tampering. Finally, a road map for secure heterogeneous integration is developed for the security research group and industry towards the secure heterogeneous integration of chiplets.

VIII. Acknowledgement

This work is partly sponsored by the Office of Naval Research (ONR) under grants N00014-21-1-2513 and N00014-22-1-2560.

References

[1] Dcadmin, "2015 international technology roadmap for semiconductors (itrs)," Sep 2018. [Online]. Available: https://www.semiconductors.org/resources/2015-international-technology-roadmap-for-semiconductors-itrs/

[2] "Universal Chiplet Interconnect Express (UCIe) Building an open chiplet ecosystem." [Online]. Available: https://www.uciexpress.org/general-8

[3] G. Keeler, S. Shumarayev, M. Wade, and B. Hamilton, *ERI Summit*. [Online]. Available: https://eri-summit.darpa.mil/2020-Agenda

[4] "Quantum effects at 7/5nm and beyond," Feb 2019. [Online]. Available: https://semiengineering.com/quantum-effects-at-7-5nm/

[5] T. Uhrmann, J. Burggraf, and M. Eibelhuber, "Heterogeneous integration by collective die-to-wafer bonding," *2018 International Wafer Level Packaging Conference (IWLPC)*, 2018.

[6] K. Yang, T. Wu, W. Chiou, M. Chen, Y. Lin, F. Tsai, C. Hsieh, C. Chang, W. Wu, Y. Chen, T. Chen, H. Wang, I. Lin, S. Jan, R. Wang, Y. Lu, Y. Shih, H. Teng, C. Tsai, M. Chang, K. Chen, S. Hou, S. Jeng, and C. Yu, "Yield and reliability of 3dic technology for advanced 28nm node and beyond," in *2011 Symposium on VLSI Technology - Digest of Technical Papers*, 2011, pp. 140–141.

[7] T. Li, J. Hou, J. Yan, R. Liu, H. Yang, and Z. Sun, "Chiplet heterogeneous integration technology—status and challenges," *Electronics*, vol. 9, no. 4, p. 670, 2020.

[8] R. Chau, "Process and packaging innovations for moore's law continuation and beyond," *2019 IEEE International Electron Devices Meeting (IEDM)*, 2019.

[9] T. Li, J. Hou, J. Yan, R. Liu, H. Yang, and Z. Sun, "Chiplet heterogeneous integration technology—status and challenges," *Electronics*, vol. 9, no. 4, 2020. [Online]. Available: https://www.mdpi.com/2079-9292/9/4/670

[10] B. Bailey, "Waiting for chiplet interfaces," Jun 2019. [Online]. Available: https://semiengineering.com/waiting-for-chiplet-interfaces/

[11] IEEE, "Chapter 20 ieee heterogeneous integration road map for thermal." [Online]. Available: https://eps.ieee.org/images/files/HIR_2019/HIR1_ch20-thermal.pdf

[12] K. Ahi, N. Asadizanjani, S. Shahbazmohamadi, M. Tehranipoor, and M. Anwar, "Terahertz characterization of electronic components and comparison of terahertz imaging with x-ray imaging techniques," in *Terahertz Physics, Devices, and Systems IX: Advanced Applications in Industry and Defense*, vol. 9483. International Society for Optics and Photonics, 2015, p. 94830K.

[13] J. True, C. Xi, N. Jessurun, K. Ahi, M. Tehranipoor, and N. Asadizanjani, "Terahertz based machine learning approach to integrated circuit assurance," in *2021 IEEE 71st Electronic Components and Technology Conference (ECTC)*. IEEE, 2021, pp. 2235–2245.

[14] T. Li, J. Hou, J. Yan, R. Liu, H. Yang, and Z. Sun, "Chiplet heterogeneous integration technology—status and challenges," *Electronics*, vol. 9, no. 4, p. 670, 2020.

[15] [Online]. Available: https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/accelerating-innovation-through-aib-whitepaper.pdf

[16] "trusted and assured microelectronics." [Online]. Available: https://rt.cto.mil/ddre-rt/dd-rtl/tam/

[17] "State of the art (sota) heterogeneous integrated packaging (ship) program." [Online]. Available: https://www.ndia.org/events/2021/12/14/287m-ship-day

[18] Intel-Newsroom, "Intel wins us government advanced packaging project." [Online]. Available: https://www.intel.com/content/www/us/en/newsroom/news/us-government-advanced-packaging-project.html

[19] "Diverse accessible heterogeneous integration." [Online]. Available: https://www.darpa.mil/program/diverse-accessible-heterogeneous-integration

[20] D. G. Keeler, "Common heterogeneous integration and ip reuse strategies (chips)." [Online]. Available: https://www.darpa.mil/program/common-heterogeneous-integration-and-ip-reuse-strategies

[21] S. Sinha, "State of iot 2021: Number of connected iot devices growing 912.3 billion globally, cellular iot now surpassing 2 billion," Sep 2021. [Online]. Available: https://iot-analytics.com/number-connected-iot-devices/

[22] "Chapter 4: Medical, health and wearables," Jan 2021. [Online]. Available: https://eps.ieee.org/images/files/HIR_2020/ch04_health.pdf

[23] "Chapter 5: Automotive - ieee electronics packaging society," Oct 2019. [Online]. Available: https://eps.ieee.org/images/files/HIR_2019/HIR1_ch05_automotive.pdf

[24] M. Deo, "Enabling next-generation platforms using intel's 3d system-in-package technology," *White Paper*, pp. 1–7, 2017.

[25] N. Vashistha, M. M. Hossain, M. R. Shahriar, F. Farahmandi, F. Rahman, and M. Tehranipoor, "echain: A blockchain-enabled ecosystem for electronic device authenticity verification," *IEEE Transactions on Consumer Electronics*, 2021.

[26] S. Bhunia and M. Tehranipoor, *Hardware security: a hands-on learning approach*. Morgan Kaufmann, 2018.

[27] J. Wurm, Y. Jin, Y. Liu, S. Hu, K. Heffner, F. Rahman, and M. Tehranipoor, "Introduction to cyber-physical system security: A cross-layer perspective," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 3, no. 3, pp. 215–227, 2016.

[28] N. Vashistha, M. T. Rahman, H. Shen, D. L. Woodard, N. Asadizanjani, and M. Tehranipoor, "Detecting hardware trojans inserted by untrusted foundry using physical inspection and advanced image processing," *Journal of Hardware and Systems Security*, vol. 2, no. 4, pp. 333–344, 2018.

[29] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor, "Hardware trojans: Lessons learned after one decade of research," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 22, no. 1, pp. 1–23, 2016.

[30] N. Vashistha, H. Lu, Q. Shi, M. T. Rahman, H. Shen, D. L. Woodard, N. Asadizanjani, and M. Tehranipoor, "Trojan scanner: Detecting hardware trojans with rapid sem imaging combined with image processing and machine learning," in *ISTFA 2018: Proceedings from the 44th International Symposium for Testing and Failure Analysis*. ASM International, 2018, p. 256.

[31] T. Meade, Y. Jin, M. Tehranipoor, and S. Zhang, "Gate-level netlist reverse engineering for hardware security: Control logic register identification," in *2016 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2016, pp. 1334–1337.

[32] S. Chen, J. Chen, D. Forte, J. Di, M. Tehranipoor, and L. Wang, "Chip-level anti-reverse engineering using transformable interconnects," in *2015 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS)*. IEEE, 2015, pp. 109–114.

[33] S. E. Quadir, J. Chen, D. Forte, N. Asadizanjani, S. Shahbazmohamadi, L. Wang, J. Chandy, and M. Tehranipoor, "A survey on chip to system reverse engineering," *ACM journal on emerging technologies in computing systems (JETC)*, vol. 13, no. 1, pp. 1–34, 2016.

[34] U. Commerce, "Defense industrial base assessment: Counterfeit electronics," *Bureau of Industry and Security, Office of Technology Evaluation, Tech. Rep*, 2010.

[35] M. Tehranipoor, H. Salmani, and X. Zhang, "Integrated circuit authentication," *Switzerland: Springer, Cham. doi*, vol. 10, pp. 978–3, 2014.

[36] M. M. Tehranipoor, U. Guin, and D. Forte, "Counterfeit integrated circuits," in *Counterfeit Integrated Circuits*. Springer, 2015, pp. 15–36.

[37] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1207–1228, 2014.

[38] U. Guin, D. DiMase, and M. Tehranipoor, "A comprehensive framework for counterfeit defect coverage analysis and detection assessment," *Journal of Electronic Testing*, vol. 30, no. 1, pp. 25–40, 2014.

[39] N. Asadizanjani, M. T. Rahman, M. Tehranipoor, and M. H. Tehranipoor, *Physical Assurance: For Electronic Devices and Systems*. Springer, 2021.

[40] M. M. Tehranipoor, H. Shen, N. Vashistha, N. Asadizanjani, M. T. Rahman, and D. Woodard, "Hardware trojan scanner," Jun. 8 2021, uS Patent 11,030,737.

[41] Q. Shi, N. Vashistha, H. Lu, H. Shen, B. Tehranipoor, D. L. Woodard, and N. Asadizanjani, "Golden gates: A new hybrid approach for rapid hardware trojan detection using testing and imaging," in *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2019, pp. 61–71.

[42] N. Vashistha, H. Lu, Q. Shi, D. L. Woodard, N. Asadizanjani, and M. Tehranipoor, "Detecting hardware trojans using combined self testing and imaging," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2021.

[43] M. T. Rahman, M. S. Rahman, H. Wang, S. Tajik, W. Khalil, F. Farahmandi, D. Forte, N. Asadizanjani, and M. Tehranipoor, "Defense-in-depth: A recipe for logic locking to prevail," *Integration*, vol. 72, pp. 39–57, 2020.

[44] "Ieee recommended practice for encryption and management of electronic design intellectual property (ip)," *IEEE Std 1735-2014 (Incorporates IEEE Std 1735-2014/Cor 1-2015)*, pp. 1–90, 2015.

[45] S. Mangard, E. Oswald, and T. Popp, *Power analysis attacks: Revealing the secrets of smart cards*. Springer Science & Business Media, 2008, vol. 31.

[46] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards sound approaches to counteract power-analysis attacks," in *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, ser. Lecture Notes in Computer Science, vol. 1666. Springer, 1999, pp. 398–412.

[47] E. Amini, A. Beyreuther, N. Herfurth, A. Steigert, B. Szyszka, and C. Boit, "Assessment of a chip backside protection," *Journal of Hardware and Systems Security*, vol. 2, no. 4, pp. 345–352, 2018.

[48] N. Vashistha, M. T. Rahman, O. P. Paradis, and N. Asadizanjani, "Is backside the new backdoor in modern socs?" in *2019 IEEE International Test Conference (ITC)*. IEEE, 2019, pp. 1–10.

[49] H. Shen, N. Asadizanjani, M. Tehranipoor, and D. Forte, "Nanopyramid: An optical scrambler against backside probing attacks," in *ISTFA 2018: Proceedings from the 44th International Symposium for Testing and Failure Analysis*. ASM International, 2018, p. 280.

[50] J. H. Lau, *Heterogeneous integrations*. Springer, 2019.

[51] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE design & test of computers*, vol. 27, no. 1, pp. 10–25, 2010.

[52] J. H. Lau, "Advanced packaging," in *Semiconductor Advanced Packaging*. Springer, 2021, pp. 1–25.

[53] M. S. M. Khan, C. Xi, A. A. Khan, M. T. Rahman, M. M. Tehranipoor, and N. Asadizanjani, "Secure interposer-based heterogeneous integration," *IEEE Design & Test*, 2022.

[54] M. Nabeel, M. Ashraf, S. Patnaik, V. Soteriou, O. Sinanoglu, and J. Knechtel, "An interposer-based root of trust: Seize the opportunity for secure system-level integration of untrusted chiplets," 2019.

[55] P. D. Schiavone, D. Rossi, A. Di Mauro, F. K. Gürkaynak, T. Saxe, M. Wang, K. C. Yap, and L. Benini, "Arnold: An efpga-augmented risc-v soc for flexible and low-power iot end nodes," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 29, no. 4, pp. 677–690, 2021.

[56] Z. Guo, M. Tehranipoor, D. Forte, and J. Di, "Investigation of obfuscation-based anti-reverse engineering for printed circuit boards," in *Proceedings of the 52nd Annual Design Automation Conference*, 2015, pp. 1–6.

[57] M. Nabeel, M. Ashraf, S. Patnaik, V. Soteriou, O. Sinanoglu, and J. Knechtel, "2.5d root of trust: Secure system-level integration of untrusted chiplets," *IEEE Transactions on Computers*, vol. 69, no. 11, pp. 1611–1625, 2020.

[58] J. Park, N. N. Anandakumar, D. Saha, D. Mehta, N. Pundir, F. Rahman, F. Farahmandi, and M. M. Tehranipoor, "Pqc-sep: Power side-channel

evaluation platform for post-quantum cryptography algorithms." *IACR Cryptol. ePrint Arch.*, vol. 2022, p. 527, 2022.

[59] B. Ahmed, M. K. Bepary, N. Pundir, M. Borza, O. Raikhman, A. Garg, D. Donchin, A. Cron, M. A. Abdel-moneum, F. Farahmandi *et al.*, "Quantifiable assurance: From ips to platforms," *arXiv preprint arXiv:2204.07909*, 2022.

[60] Y. Xie, C. Bao, C. Serafy, T. Lu, A. Srivastava, and M. Tehranipoor, "Security and vulnerability implications of 3d ics," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 2, no. 2, pp. 108–122, 2016.

[61] H. Wang, D. Forte, M. M. Tehranipoor, and Q. Shi, "Probing attacks on integrated circuits: Challenges and research opportunities," *IEEE Design & Test*, vol. 34, no. 5, pp. 63–71, 2017.

[62] H. Wang, Q. Shi, A. Nahiyan, D. Forte, and M. M. Tehranipoor, "A physical design flow against front-side probing attacks by internal shielding," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, no. 10, pp. 2152–2165, 2019.

[63] H. Wang, Q. Shi, D. Forte, and M. M. Tehranipoor, "Probing assessment framework and evaluation of antiprobing solutions," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 6, pp. 1239–1252, 2019.

[64] J. Dofe, P. Gu, D. Stow, Q. Yu, E. Kursun, and Y. Xie, "Security threats and countermeasures in three-dimensional integrated circuits," in *Proceedings of the on Great Lakes Symposium on VLSI 2017*, 2017, pp. 321–326.

[65] [Online]. Available: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html

[66] [Online]. Available: https://www.sungardas.com/en-us/blog/ransomware-attacks-on-us-government-entities/

[67] [Online]. Available: https:https://www.cybersecuritydive.com/news/ransomware-attacks-payouts-2021/622784/

[68] N. Farzana, F. Rahman, M. Tehranipoor, and F. Farahmandi, "Soc security verification using property checking," in *2019 IEEE International Test Conference (ITC)*, 2019, pp. 1–10.

[69] G. K. Contreras, M. T. Rahman, and M. Tehranipoor, "Secure split-test for preventing ic piracy by untrusted foundry and assembly," in *2013 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS)*, 2013, pp. 196–203.

[70] U. Guin, D. Forte, and M. Tehranipoor, "Design of accurate low-cost on-chip structures for protecting integrated circuits against recycling," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 24, no. 4, pp. 1233–1246, 2015.

[71] X. Xu, F. Rahman, B. Shakya, A. Vassilev, D. Forte, and M. Tehranipoor, "Electronics supply chain integrity enabled by blockchain," *ACM Transactions on Design Automation of Electronic Systems*, vol. 24, no. 3, p. 1–25, 2019.

[72] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[73] "IEEE Standard for Test Access Architecture for Three-Dimensional Stacked Integrated Circuits ," *IEEE Std 1838-2019*, pp. 1–73, 2020.

[74] "Heterogeneous Integrated Product Testability Best-Known Methods (BKM)." [Online]. Available: https://cmte.ieee.org/eps-test/wp-content/uploads/sites/132/2022/01/IEEE_EPS_Test_Het_Int_Product_Testability_BKM_Final_v1_0-1-14-22-1.pdf

[75] M. R. Muttaki, M. Tehranipoor, and F. Farahmandi, "FTC: A universal fault injection attack detection sensor," in *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. IEEE, 2022.

[76] A. Mazumder Shuvo, N. Pundir, J. Park, F. Farahmandi, and M. Tehranipoor, "LDTFI: Layout-aware timing fault-injection attack assessment against differential fault analysis," in *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE, 2022.

[77] H. Igarashi, Y. Shi, M. Yanagisawa, and N. Togawa, "Concurrent faulty clock detection for crypto circuits against clock glitch based dfa," in *2013 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2013, pp. 1432–1435.

[78] S. Paley, T. Hoque, and S. Bhunia, "Active protection against pcb physical tampering," in *2016 17th International Symposium on Quality Electronic Design (ISQED)*. IEEE, 2016, pp. 356–361.

[79] N. Patel, A. Sasan, and H. Homayoun, "Analyzing hardware based malware detectors," in *2017 54th ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2017, pp. 1–6.

[80] N. Pundir, M. M. Tehranipoor, and F. Rahman, "Ranstop: A hardware-assisted runtime crypto-ransomware detection technique," *ArXiv*, vol. abs/2011.12248, 2020.

[81] B. Zhou, A. Gupta, R. Jahanshahi, M. Egele, and A. Joshi, "Hardware performance counters can detect malware: Myth or fact?" in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, ser. ASIACCS '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 457–468. [Online]. Available: https://doi.org/10.1145/3196494.3196515

[82] M. Zhao and G. E. Suh, "Fpga-based remote power side-channel attacks," in *2018 IEEE Symposium on Security and Privacy (SP)*, 2018, pp. 229–244.

[83] T. Eisenbarth, C. Paar, and B. Weghenkel, "Building a side channel based disassembler," in *Transactions on computational science X*. Springer, 2010, pp. 78–99.

[84] J. Park, X. Xu, Y. Jin, D. Forte, and M. Tehranipoor, "Power-based side-channel instruction-level disassembler," in *2018 55th ACM/ESDA/IEEE Design Automation Conference (DAC)*, 2018, pp. 1–6.

[85] Z. Pan, J. Sheldon, C. Sudusinghe, S. Charles, and P. Mishra, "Hardware-assisted malware detection using machine learning," in *2021 Design, Automation Test in Europe Conference Exhibition (DATE)*, 2021, pp. 1775–1780.

[86] F. Kenarangi and I. Partin-Vaisband, "Exploiting machine learning against on-chip power analysis attacks: Tradeoffs and design considerations," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 2, pp. 769–781, 2019.

[87] S. Ray, E. Peeters, M. M. Tehranipoor, and S. Bhunia, "System-on-chip platform security assurance: Architecture and validation," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 21–37, 2018.

[88] S. Ray and Y. Jin, "Security policy enforcement in modern soc designs," in *2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2015, pp. 345–350.

[89] B. Ahmed, F. Rahman, N. Hooten, F. Farahmandi, and M. Tehranipoor, "AutoMap: Automated Mapping of Security Properties Between Different Levels of Abstraction in Design Flow," in *2021 IEEE/ACM International Conference On Computer Aided Design (ICCAD)*, 2021, pp. 1–9.

[90] N. Vashistha, M. M. Al Hasan, N. Asadizanjani, F. Rahman, and M. Tehranipoor, "Trust validation of chiplets using a physical inspection based certification authority," in *2022 IEEE 72nd Electronic Components and Technology Conference (ECTC)*. IEEE, 2022, pp. 2311–2320.

[91] G. E. Suh, D. Clarke, B. Gassend, M. Van Dijk, and S. Devadas, "Aegis: Architecture for tamper-evident and tamper-resistant processing," in *ACM International Conference on Supercomputing 25th Anniversary Volume*, 2003, pp. 357–368.

[92] W. Arthur, D. Challener, and K. Goldman, *A practical guide to TPM 2.0: Using the new trusted platform module in the new age of security*. Springer Nature, 2015.

[93] A. Arm, "Security technology-building a secure system using trustzone technology," *ARM Technical White Paper*, 2009.

[94] F. McKeen, I. Alexandrovich, A. Berenzon, C. V. Rozas, H. Shafi, V. Shanbhogue, and U. R. Savagaonkar, "Innovative instructions and software model for isolated execution." *Hasp@ isca*, vol. 10, no. 1, 2013.

[95] D. Champagne and R. B. Lee, "Scalable architectural support for trusted software," in *HPCA-16 2010 The Sixteenth International Symposium on High-Performance Computer Architecture*. IEEE, 2010, pp. 1–12.

[96] J. Noorman, P. Agten, W. Daniels, R. Strackx, A. Van Herrewege, C. Huygens, B. Preneel, I. Verbauwhede, and F. Piessens, "Sancus: Low-cost trustworthy extensible networked devices with a zero-software trusted computing base," in *22nd {USENIX} Security Symposium ({USENIX} Security 13)*, 2013, pp. 479–498.

[97] F. Brasser, B. El Mahjoub, A.-R. Sadeghi, C. Wachsmann, and P. Koeberl, "Tytan: Tiny trust anchor for tiny devices," in *Proceedings of the 52nd annual design automation conference*, 2015, pp. 1–6.

[98] M. S. U. I. Sami, F. Rahman, F. Farahmandi, A. Cron, M. Borza, and M. Tehranipoor, "End-to-end secure soc lifecycle management," in *2021 58th ACM/IEEE Design Automation Conference (DAC)*. IEEE, 2021, pp. 1295–1298.

[99] M. S. U. I. Sami, F. Rahman, A. Cron, D. Donchin, M. Borza, F. Farahmandi, and M. Tehranipoor, "Poca: First power-on chip authentication in untrusted foundry and assembly," in *2021 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2021, pp. 124–135.

[100] M. M. Hossain, N. Vashistha, J. Allen, M. Allen, F. Farahmandi, F. Rahman, and M. Tehranipoor, "Thwarting counterfeit electronics by blockchain," 2022.

Nidish Vashistha (S'09) received his MS (2015) in electrical and computer engineering from the University of Florida. He is currently a Ph.D. candidate at the Florida Institute for Cybersecurity Research (FICS) within the Electrical and Computer Engineering (ECE) Department at the University of Florida. His previous work experience includes Yield Enhancement and Physical Failure Analysis intern at Micron. Earlier, he worked at Renesas Electronics America as a Product and Test Engineering intern and an RF engineer at Ericsson. He is a reviewer for IEEE Transactions on Circuits and Systems I: Regular Papers and Springer's Journal of Hardware and Systems Security. His research interests include secure electronic circuits design and trust validation using SEM nano-imaging, computer vision, and machine learning.

Md Latifur Rahman received his BS in electrical and electronic engineering from Bangladesh University of Engineering and Technology, Bangladesh. He is currently a Ph.D. student at the Florida Institute for Cybersecurity Research (FICS) within the Electrical and Computer Engineering (ECE) Department at the University of Florida. His research focuses on secure heterogeneous integration, post-quantum cryptography, and side channel attacks.

Md Saad Ul Haque received his BS in electrical and electronic engineering from Bangladesh University of Engineering and Technology. He is currently a Ph.D. student at the Florida Institute for Cybersecurity Research (FICS) within the Electrical and Computer Engineering (ECE) Department at the University of Florida.. His research focuses on secure electronic system design and trust validation.

Azim Uddin received his BSc in Electrical and Electronics Engineering from Bangladesh University of Engineering and Technology. He is currently a Ph.D. student at the Florida Institute for Cybersecurity Research (FICS) within the Electrical and Computer Engineering (ECE) Department at the University of Florida. His research focuses on secure system-on-chips (SoCs) and internet-of-things (IoT) security.

Amit Mazumder Shuvo received his BSc in Electrical and Electronic Engineering from Bangladesh University of Engineering and Technology. He is currently a Ph.D. student and a graduate research assistant at the Florida Institute for Cybersecurity Research (FICS) within the Electrical and Computer Engineering (ECE) Department at the University of Florida. His research focuses on fault injection attack assessment, tamper detection, and secure heterogeneous integration.

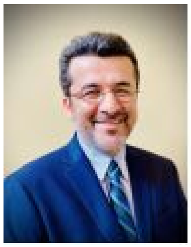
Md Sami Ul Islam Sami received his BSc in Electrical and Electronic Engineering (EEE) from Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh. He is currently a Ph.D. student and a graduate research assistant at the Florida Institute for Cybersecurity Research (FICS) within the Electrical and Computer Engineering (ECE) Department at the University of Florida. His research focuses on hardware security and trust, secure SoC design, hardware-based security protocol design, and VLSI.

Paul Calzada received his BS in computer engineering from the University of Florida (UF). He is currently a Ph.D. student at the Florida Institute for Cybersecurity Research (FICS) within the Electrical and Computer Engineering (ECE) Department at the University of Florida. His research focuses on hardware security and trust, secure heterogeneous integration, and PCB-level Trojans.

Farimah Farahmandi (S'13-M'18) is an Assistant Professor in the Department of Electrical and Computer Engineering (ECE) at the University of Florida (UF). She received her Ph.D. from the Department of Computer and Information Science and Engineering (CISE) at the University of Florida 2018. She received her B.Sc. and M.Sc. from the Department of Computer Engineering at the University of Tehran, Tehran, Iran, in 2010 and 2013, respectively. Her research interests include design automation of System-on-Chips and energy-efficient systems, formal verification, hardware security validation, and post-silicon validation and debug. Her research has been sponsored by SRC, DARPA, AFRL, DoD, Analog Devices, Ansys, and Cisco. Dr. Farahmandi is currently the associate director of Edaptive Computing Inc, Transition Center (ECI-TC) at the University of Florida.

Navid Asadizanjani received the Ph.D. degree in Mechanical Engineering from University of Connecticut, Storrs, CT, USA, in 2014. He is currently an Assistant Professor with the Electrical and Computer Engineering Department at University of Florida, Gainesville, FL, USA. His current research interest is primary on "Physical Assurance and Inspection of Electronics". This includes wide range of products from electronic systems to devices. He is involved with counterfeit detection and prevention, system and chip level reverse engineering, Anti reverse engineering, etc. Dr. Asadizanjani has received and nominated for several best paper awards from International Symposium on Hardware Oriented Security and Trust (HOST) and International Symposium on Flexible Automation (ISFA). He was also winner of D.E. Crow Innovation award from University of Connecticut. He is currently the program chair of the IEEE PAINE conference and is serving on the technical program committee of several top conferences including International Symposium of Testing and Failure Analysis (ISTFA) and IEEE Computing and Communication Workshop and Conference (CCWC).

Fahim Rahman (S13-M19) received his BS in electrical and electronic engineering from Bangladesh University of Engineering and Technology, Bangladesh and MS in electrical and computer engineering from the University of Connecticut, USA in 2015. He received his Ph.D. in electrical and computer engineering from the University of Florida in 2018. He is currently a Research Assistant Professor within the Electrical and Computer Engineering Department at the University of Florida. His current research interests are in the domain of hardware and cybersecurity and trust including electronic supply-chain security, CAD for security and automatic assessment, and hardware-assisted cybersecurity. His research has been sponsored by SRC, AFOSR, AFRL, DARPA, Cisco, TI, and NIST. He is a member of IEEE and ACM.



Mark M. Tehranipoor (S'02-M'04-SM'07-F'18) is currently the Intel Charles E. Young Preeminence Endowed Chair Professor in Cybersecurity and ECE Department Chair at the University of Florida. His current research projects include: hardware security and trust, supply chain security, IoT security, VLSI design, test, and reliability. Dr. Tehranipoor has published over 500 journal articles and referenced conference papers, has delivered many talks, and has published 13 books. He is a recipient of a dozen best paper awards and nominations, as well as the 2008 IEEE Computer Society (CS) Meritorious Service Award, the 2012 IEEE CS Outstanding Contribution, the 2009 NSF CAREER Award, and the 2014 AFOSR MURI award. He received the 2020 University of Florida Innovation of the Year award. He serves on the program committee of more than a dozen leading conferences and workshops. He has also served as program chair of a number of IEEE and ACM-sponsored conferences and workshops (HOST, ITC, DFT, D3T, DBT, NATW, and more). He co-founded the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) and served as HOST-2008 and HOST-2009 General Chair. He is currently serving as a founding EIC for Journal on Hardware and Systems Security (HaSS) and Associate Editor for JETTA, JOLPE, IEEE TVLSI, and ACM TODAES. Before joining UF, Dr. Tehranipoor served as the founding director for CHASE and CSI centers at the University of Connecticut. He is currently serving as a founding director for the Florida Institute for Cybersecurity Research (FICS). Dr. Tehranipoor is a fellow of the IEEE, a golden core member of IEEE CS, and a member of ACM and ACM SIGDA.