Securing the Interconnect in Heterogeneous 3DICs: Threats and Emerging Solutions

Dipal Halder and Sandip Ray
Electrical and Computer Engineering, University of Florida, Gainesville, FL, USA
{dipal.halder, sandip}@ece.ufl.edu

2025 IEEE 34st Microelectronics Design & Test Symposium (MDTS) | 979-8-3315-3689-3/25/$31.00 ©2025 IEEE | DOI: 10.1109/MDTS64924.2025.11177065

***Abstract*—Heterogeneous integration in modern semiconductor design is propelling the adoption of 2.5D and 3D integrated circuits, where diverse chiplets—ranging from CPUs and GPUs to specialized accelerators and memory—coexist on a single package. Although this approach promises remarkable gains in performance, power efficiency, and scalability, it also introduces critical vulnerabilities at the *3D interconnect* that ties these chiplets together. In this invited paper, we show how adversaries can exploit both *intra-chiplet* and *inter-chiplet* communication through supply-chain tampering, Trojan insertion, reverse engineering, and side-channel techniques. We define a broad threat model emphasizing the centrality of interconnect security in heterogeneous 3D architectures, revealing how a single untrusted chiplet or compromised interposer can undermine the entire system. Finally, we stress the need for *holistic* solutions—encompassing secure chiplet authentication, in-field monitoring, and rigorous supply-chain validation—to ensure that the performance benefits of 3D packaging do not come at the cost of trust.**

***Index Terms*—3DIC, chiplet security, interconnect security, hardware security**

I. Introduction

The semiconductor industry has recently seen a notable shift toward integrating multiple independently manufactured *chiplets* into a single package, often through 2.5D or 3D integrated circuit (**3DIC**) technology. Rather than placing every component on one large die, designers now combine specialized, known-good dies—ranging from CPUs and GPUs to memory and AI accelerators—on a shared interposer or by vertically stacking them with through-silicon vias (TSVs). This strategy aims to balance performance, power, and flexibility: for instance, a proven memory chiplet might be fabricated in a mature node, while a more advanced node can be reserved for high-performance compute chiplets 1.

Of course, the move to heterogeneous integration raises important security questions. Conventional SoC security research frequently addresses threats like hardware Trojans, reverse engineering, side-channel leakage, and intellectual property (IP) piracy. In a 3D system, however, these issues can escalate. Not only do attackers gain more potential entry points—such as the vertical interconnects or the interposer's routing—but the overall supply chain also becomes more intricate [1]. When designers source different chiplets from various vendors, any one of those dies could be compromised or malicious. In the worst case, an untrusted chiplet might inject harmful payloads or stealthily siphon data across the stacked layers [2].

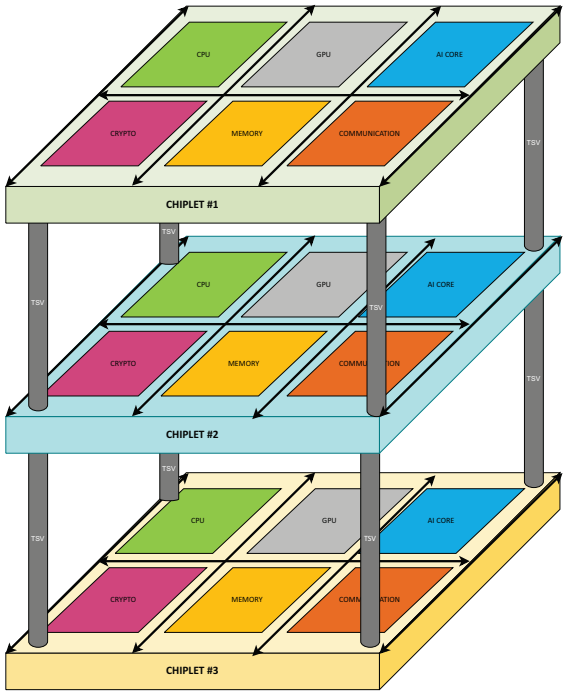

Fig. 1. Heterogeneous 3DIC with multiple specialized chiplets.

Among the different components in a 3D package, the *interconnect fabric*—whether on an interposer or through TSVs—deserves special attention. It essentially acts like a data highway, shuttling information between logic, memory, and specialized accelerators. If an adversary succeeds in tapping or modifying these connections, the consequences could be serious: leaked secrets, tampered computations, or disruption of system reliability. Compounding this concern, it is often harder to inspect the internal layers of a 3D design, so detecting malicious changes is more challenging than in a traditional 2D SoC.

In response, researchers have started to propose new countermeasures that address threats unique to 3D packaging. Examples include authenticating chiplets before assembly, deploying secure root-of-trust hardware in the interposer, and adding built-in self-test or real-time monitoring features that watch for suspicious behavior within the stack [3]. Another emerging idea is *dynamic (or reconfigurable) obfuscation*,

which involves periodically changing how data travels across the 3D interconnect so attackers cannot easily track a stable route or predict signal behavior over time. Such an approach may complicate reverse engineering and thwart hardware Trojans that rely on predictable data patterns.

In this paper, we focus on *interconnect security* in 3DICs and introduce the idea of dynamic obfuscation as a high-level strategy to make unauthorized access or manipulation significantly harder. We start by identifying the key gaps that arise when scaling SoC security approaches into 3D environments, then move on to a broad threat model covering both supply-chain and runtime attacks. We conclude by outlining how a reconfigurable approach to obfuscation can defend against these threats, while also discussing practical hurdles and open questions. Our hope is that, by treating interconnect security as central rather than secondary, future 3D systems can fully leverage their performance benefits without sacrificing trust.

II. Research Gap and Motivation

Over the last two decades, hardware security research has largely centered on *planar (2D) SoC* challenges, focusing on IP protection, reverse engineering countermeasures, side-channel mitigation, and supply-chain validation. Many of these approaches assume a relatively uniform manufacturing flow—one where all core components are integrated on a single silicon die and verified through conventional design-time or post-silicon methods.

However, heterogeneous integration of *3D integrated circuits (3DICs)* upends this model. Multiple chiplets may be sourced from different vendors, stacked together vertically or assembled on an interposer, and interconnected through high-density interfaces like TSVs or UCIe. While this 3D paradigm delivers significant performance and cost advantages, it also exposes new attack surfaces. The stacked layers are harder to inspect, supply chains become more fragmented, and cross-die phenomena introduce unique vulnerabilities [4].

A. High-Level Review of Existing Work

Despite substantial progress in hardware security, most solutions address either:

1) **2D SoC-centric approaches**: Techniques such as logic locking, static obfuscation, or IP watermarking typically presume a single-plane design.
2) **Partial 3D security measures**: A few studies consider supply-chain threats for 2.5D or 3D packaging, but often emphasize verifying chiplet authenticity rather than systematically protecting the shared interconnect fabric [5], [6].

Furthermore, side-channel research in 3D contexts often shows that stacking exacerbates thermal and power-based leakages, but seldom details how to *practically* monitor these leaks at runtime across multiple tiers. Meanwhile, work on *reverse engineering prevention* typically targets individual chiplets rather than the *vertically integrated interconnect fabric* itself.

In short, few solutions offer a *comprehensive security framework* specifically tailored for protecting the *3D interconnect*—the data "backbone" tying together these heterogeneous chiplets. Conventional encryption or obfuscation methods, designed with a planar SoC in mind, may struggle to scale up to the layered routing, diverse ownership models, and multi-tier test complexities of 3DICs.

B. Key Gaps in 3D Interconnect Security

a) Runtime Monitoring in Stacked Architectures: Conventional NoC-based monitors rely on easy visibility and control signals that simply do not exist in many 3D deployments. Vertical links can hide Trojan activations, anomalies, or data breaches from standard 2D debugging approaches.

b) Supply-Chain Threats in Heterogeneous Chiplets: Once multiple chiplets—possibly with different trust levels—are brought together, a single maliciously crafted chiplet can compromise the entire interconnect. Existing authenticity checks do not always extend to *in-field exploitation*, where a Trojan can remain dormant until specific conditions in a 3D stack arise.

c) Trojan Insertion in Interposer/TSVs: Although hardware Trojans in 2D SoCs have been studied extensively, comparatively little research addresses hidden modifications designed to exploit the *layered nature* of 3D integration. Trojans placed in the interposer or connected via TSVs can intercept or corrupt communication across multiple stacked tiers, often evading post-silicon tests.

C. Why Now?

Mainstream adoption of *heterogeneous 3D packaging* is no longer speculative. The emergence of "chiplet marketplaces" (as seen with DARPA's CHIPS program, AMD's multi-die GPUs, or Intel's Foveros technology) is rapidly expanding. Unfortunately, most design-time and in-field security methods remain anchored in *2D SoC* assumptions, providing incomplete defenses against the multi-tier complexity of 3D systems. Addressing these gaps is essential to ensure that 3DICs can achieve their performance and cost benefits without sacrificing security.

III. 3DIC Versus 2D SoC Interconnect Security: Key Differences

While 2D hardware security research offers a valuable starting point, *3D integration* introduces key architectural, physical, and supply-chain differences that render many traditional solutions inadequate. Below, we highlight the major contrasts and their implications for interconnect security.

A. Physical and Topological Complexity

In a 2D SoC, IP blocks lie on a single layer of silicon, with well-established metal routing and debug interfaces. By contrast, 3DICs leverage vertical stacking through TSVs or advanced interposers, creating:

- **Obscured Internal Layers:** Subsurface dies are challenging to inspect non-destructively, enabling stealthy Trojan insertion or tampering.

- **Layered Testing Barriers:** Traditional debug or scan architectures may not extend seamlessly across multiple stacked tiers, complicating post-fabrication validation.

B. Heterogeneous Chiplet Ecosystem

In a planar SoC flow, all components typically share a single fabrication process and security baseline. A 3D system, however, might integrate CPU, GPU, memory, and AI accelerators from different vendors or nodes. This leads to:

- **Mixed Trust Levels:** A single compromised chiplet can undermine the entire 3D package.
- **Diverse Security Standards:** Disparate encryption, authentication, or obfuscation approaches across chiplets leave gaps for attackers to exploit.

C. Amplified Side-Channel Exposure

While 2D SoCs are not immune to side-channel attacks (e.g., power or EM analysis), 3DICs can exacerbate these threats by placing multiple active layers in close proximity:

- **Thermal Coupling:** An attacker can track heat signatures of a security-critical die from a neighboring layer.
- **Power Network Overlaps:** Voltage glitching or advanced differential analysis becomes more feasible when multiple dies share tight power rails.

Solutions designed for planar SoCs may fail to handle these intensified cross-tier effects.

D. New Trojan Trigger Conditions

Many 2D Trojans rely on rarely used signals or debug ports. In a 3D stack, Trojans can exploit:

- **Vertical Inconsistencies:** Temperature or voltage anomalies unique to stacked layers.
- **Cross-Die Transactions:** Specialized chiplet-to-chiplet protocols may serve as stealthy triggers for malicious behavior.

E. More Opaque Supply Chains

A 2D SoC is often built at a single foundry. In 3D, multiple foundries or assembly houses may each handle different parts (chiplets, interposer, bonding). Trust must be verified at every stage, but oversight is inherently harder in a fragmented manufacturing pipeline.

F. Implications for Secure 3D Interconnect Design

Traditional SoC security approaches (e.g., static obfuscation, single-plane bus encryption) struggle to account for the multi-tier arrangement, cross-tier side channels, and multi-vendor complexity of 3D. A robust *3DIC security* methodology must:

- **Adapt to Layered Verification:** Provide new ways to inspect deeper layers and detect tampering within the interposer or TSV routing.
- **Address Mixed Trust Levels:** Enforce authentication and secure handshakes in both *intra-* and *inter-chiplet* communication.

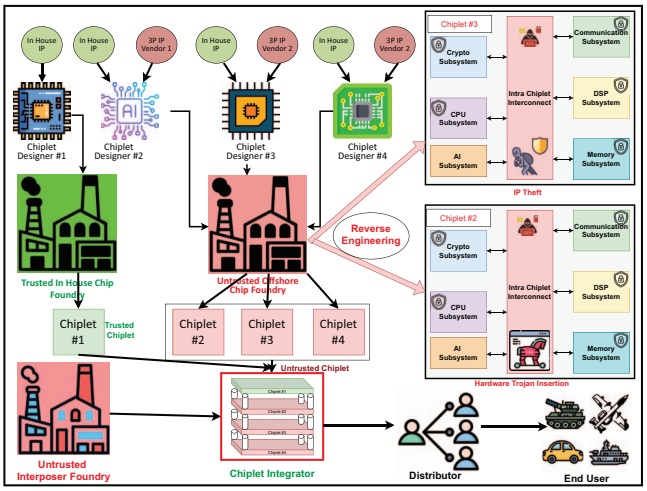

Fig. 2. Attack Model in a Multi-Chiplet Ecosystem. Various foundries, 3P IP vendors, and integration facilities introduce multiple points of vulnerability.

- **Mitigate Cross-Tier Side-Channels:** Incorporate thermal/power balancing, noise injection, or dynamic reconfiguration to thwart advanced side-channel exploitation.

G. Attack Model in a Multi-Chiplet Ecosystem

Figure 2 illustrates a representative multi-tier supply chain for a chiplet-based 3D system. Multiple chiplet designers, third-party IP (3P IP) vendors, and offshore foundries contribute to individual dies, which are then assembled on an interposer by a chiplet integrator. This network of actors introduces numerous points of vulnerability that adversaries can exploit to compromise the final product:

- **Chiplet Designers and 3P IP Vendors:** Each chiplet may integrate a mix of in-house IP and third-party IP from different vendors. An attacker could inject malicious logic or leak sensitive design details during IP licensing or SoC integration stages. If a chiplet designer is untrusted, Trojan insertion or backdoor creation becomes a risk.
- **Offshore Foundries (Untrusted Fabrication):** While some chiplets might be fabricated in trusted in-house facilities, others could be sent to cost-effective offshore foundries that lack rigorous security guarantees. Here, an adversary could introduce stealthy modifications, leak proprietary layouts, or overproduce unauthorized chiplets, leading to IP theft and counterfeits.
- **Untrusted Interposer Foundry:** Even if individual chiplets are verified as secure, a malicious interposer supplier could embed Trojan circuits or reroute signals at the interposer level. Because 3D stacking often obscures deeper layers from post-assembly inspection, such tampering may remain undetected.
- **Chiplet Integration and Distribution:** The final assembly stage, where multiple chiplets are bonded together, presents another opportunity for reverse engineering or Trojan insertion—especially if the assembly house or distributor is not fully trusted. Once the packaged device

is deployed to the end user, detecting deeply hidden hardware anomalies (e.g., hidden test pins or stealthy bridging logic) can be exceedingly difficult.

- **In-Field Threats:** A compromised chiplet within the final product can intercept or manipulate intra-chiplet communication (e.g., memory subsystem or DSP subsystem) as well as inter-chiplet links (e.g., bridging between CPU and AI subsystems). Additionally, hardware Trojans might remain dormant until specific run-time conditions are met, evading conventional test flows.
- **Potential Attacks:** *IP Theft* occurs when adversaries glean proprietary design secrets (e.g., critical DSP or AI logic), while *Trojan Insertion* introduces stealthy hardware modifications that can sabotage operations or exfiltrate data post-deployment. Further vulnerabilities include reverse engineering, counterfeit reproduction, or denial-of-service against specific chiplets.

Collectively, the figure underscores the complexity of securing a 3D chiplet-based system, where each entity in the supply chain—from individual chiplet designers to interposer foundries and final integrators—can become a potential attack vector. Securing the interconnect across chiplets, validating each die, and ensuring trusted assembly are therefore paramount to safeguarding the end user against unauthorized data leaks and system manipulation.

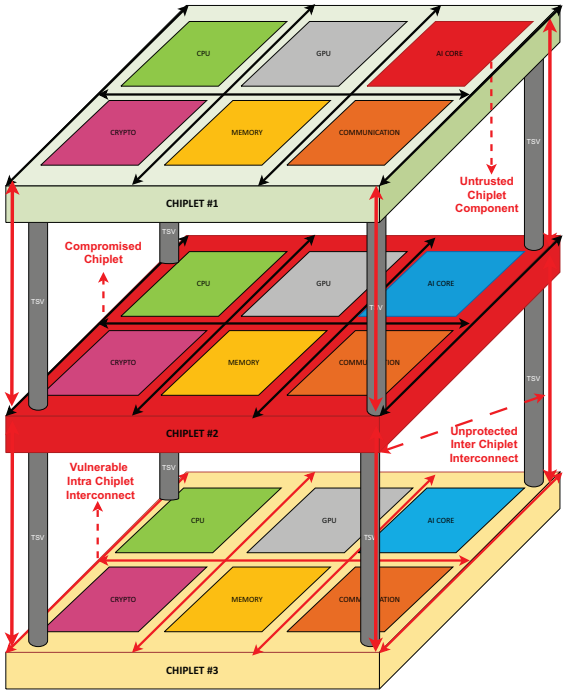

Fig. 3. Chiplet based modern microelectronic system

IV. 3DIC Interconnect Security

Modern 3D integrated circuits (3DICs) unite multiple chiplets—including CPUs, GPUs, memory, crypto accelerators, and domain-specific modules—on a shared substrate (interposer) or through stacked tiers connected by through-silicon vias (TSVs). This heterogeneous integration approach provides significant performance and flexibility gains but also amplifies security challenges. One crucial aspect is *interconnect security*: because the interconnect handles nearly all communication among chiplets, any compromise at this level can jeopardize the entire system. In the following subsections, we distinguish between *intra-chiplet* interconnects (communication *within* a chiplet) and *inter-chiplet* interconnects (communication *among* different chiplets), then discuss a threat model that encompasses both.

A. Intra- versus Inter-Chiplet Communication

a) Intra-Chiplet Interconnects: Inside each chiplet, functional units such as processors, memory controllers, accelerators, and custom IP blocks communicate over localized interconnect fabrics. These may be implemented using well-known on-chip networks, buses, or crossbars. While *intra-chiplet* security often mirrors that of traditional System-on-Chip (SoC) concerns (e.g., reverse engineering, Trojan insertion in the NoC), the **stacked layout** and close proximity of other chiplets in 3DICs can intensify side-channel and Trojan-trigger risks.

b) Inter-Chiplet Interconnects: Multiple chiplets, each potentially built in different process nodes or by different vendors, must communicate via a high-bandwidth, low-latency interface such as the Universal Chiplet Interconnect Express (UCIe) or through custom interposer routing. This *inter-chiplet* communication is especially vulnerable to malicious alterations or monitoring—a compromised chiplet or tampered interposer can eavesdrop on (or inject into) the shared data lines.

B. Threats Targeting 3D Interconnects

a) Malicious or Compromised Chiplets: In a multi-vendor ecosystem, chiplets may arrive with hidden Trojan circuitry designed to intercept or insert traffic specifically at the interconnect level. For instance, a rogue accelerator chiplet could embed stealthy logic that monitors encryption key exchanges occurring over the TSV links. Since these chiplets are often "black boxes," verifying that their internal logic does not tamper with signals can be exceedingly difficult.

b) Reverse Engineering via the Interconnect: An attacker tapping interposer lines or TSVs may passively collect traffic, reconstruct control sequences, or extract proprietary code. Intercepting part of an encrypted transaction could enable advanced attacks correlating that data with side-channel emissions in other layers.

c) Untrusted Interposer or Assembly House: Even if chiplets themselves are verified, a malicious interposer supplier might embed Trojan logic or re-route signals covertly. Similarly, a dishonest assembly house could alter TSV connections, bridging logic, or partial re-wiring. Stacked designs obscure these layers, preventing thorough post-assembly inspection.

d) Illustrative 3D Threat Scenario: Figure 3 provides a conceptual view of a heterogeneous 3D system comprising three stacked chiplets. Each chiplet integrates multiple functional blocks, such as CPUs, GPUs, cryptographic engines, AI cores, memory, and communication logic, all connected via local (*intra-chiplet*) interconnects. Vertical data exchange occurs through through-silicon vias (TSVs), and the chiplets themselves link together over *inter-chiplet* communication channels on the interposer or advanced packaging layers.

Notably, **Chiplet #2** is marked as *compromised*, highlighting how a single untrusted or maliciously modified chiplet can threaten the entire 3D package. If this chiplet contains Trojan circuits or is under adversarial control, it can exploit the *unprotected inter-chiplet interconnect* to intercept or corrupt traffic heading to or from neighboring chiplets. In parallel, the *vulnerable intra-chiplet interconnect* within Chiplet #3 underscores that even local communication (e.g., between a CPU and cryptographic module) can become a vector for attack if insufficiently secured.

- **Untrusted Components:** As shown by the "Untrusted Chiplet Component" in Chiplet #1, hardware originating from unknown or lower-trust vendors can be introduced during assembly, exposing the system to potential tampering or backdoor insertion.
- **3D-Specific Trojan Triggers:** Trojans may rely on *3D triggers* (e.g., temperature fluctuations, TSV signal patterns) to activate malicious functionality only after the device is fully stacked and operational, thus evading standard 2D test and validation procedures.
- **Cross-Chiplet Exploits:** By leveraging the high-bandwidth vertical links, a compromised chiplet can steal secrets from a cryptographic engine in another layer, inject forged data into shared memory, or disrupt system-level communication entirely.

Overall, the figure highlights how multiple attack vectors converge on the 3D interconnect: from untrusted chiplet IP blocks and Trojan-laden logic in the vertical communication paths to vulnerable intra-chiplet buses. Consequently, any *3DIC security framework* must address both local (within-chiplet) and global (cross-chiplet) communication threats, especially when the supply chain involves vendors or foundries of varying trust levels.

By targeting the interconnect, an attacker can not only gather sensitive data but also manipulate the high-bandwidth links that every chiplet relies on. In the following sections, we discuss strategies—including dynamic obfuscation—that focus on safeguarding these crucial interconnect links to ensure system integrity and confidentiality.

V. Emergent Research Directions for 3D Interconnect Security

The challenges outlined in the previous sections underscore the pressing need for new, holistic security strategies tailored to the 3D interconnect. Below, we highlight several promising directions—ranging from novel obfuscation techniques to secure chiplet authentication protocols—that could significantly enhance the resilience of future heterogeneous 3D systems.

A. Reconfigurable (Dynamic) Obfuscation

Recent work on network-on-chip (NoC) obfuscation in 2D SoCs suggests that dynamically remapping routing paths or encrypting protocol signals can effectively deter reverse engineering attacks [5], [6]. Extending these ideas to 3D chiplet environments offers a powerful deterrent: if data paths through through-silicon vias (TSVs) or interposers are reconfigured on-the-fly, adversaries lose the stable vantage points they rely on to eavesdrop or trigger malicious events. However, such reconfigurable solutions must minimize overheads in area and power while providing sufficient complexity to thwart sophisticated attackers.

In parallel, *FPGA-inspired* (or "reconfigurable-based") obfuscation approaches [7], [8]—where selected netlist portions are replaced by small LUT-based blocks and finalized only via a secure post-fabrication bitstream—can further protect 3DICs from reverse engineering or overproduction. By concealing security-critical logic behind a configurable layer, the foundry or assembly house never sees the complete functional design, undermining attempts at Trojan insertion or IP theft. As with NoC-level reconfiguration, however, designers must weigh the area, power, and performance implications of embedding LUT macros in a 3D stack, balancing the security gains with feasible overhead.

B. Integrated Root-of-Trust for Chiplet Authentication

As chiplet marketplaces mature, verifying the *authenticity* of each chiplet becomes vital. Trusted hardware modules (e.g., secure enclaves or physically unclonable functions) could be embedded in each chiplet, enabling mutual authentication at startup. Once assembled in a 3D package, these mechanisms assure that only legitimate chiplets can exchange data over the interconnect. This approach can also tie into secure boot protocols, ensuring the entire stack loads trustworthy firmware before any data exchange begins. The main challenge is balancing robust security with practical design and manufacturing constraints.

C. Run-Time Monitoring and Intrusion Detection

Traditional in-field monitoring in 2D SoCs often relies on performance counters or network traffic monitors embedded in the interconnect. In 3DICs, more advanced *runtime analysis* tools are essential to detect suspicious activity:

- **Traffic Pattern Analysis**: Profiling normal traffic flows across the interposer or TSVs, then flagging anomalies that could indicate an active Trojan or malicious chiplet.
- **Thermal/Power Sensors**: Exploiting the proximity of layers in 3D to sense cross-tier temperature or voltage fluctuations. Sudden, unexplained changes in these profiles may signal tampering or a stealthy attack.

Real-time event logging and machine learning–based anomaly detection have the potential to raise early alarms when malicious behavior surfaces.

D. EDA Tool Support and Automated Security Validation

A critical barrier to deploying advanced security measures (e.g., reconfigurable interconnects, chiplet authentication) is a lack of mature *electronic design automation (EDA)* flows that support them. Future research could focus on:

- **Security-Aware Floorplanning**: Tools that automatically place chiplets, route TSVs, and position sensitive modules to minimize side-channel leakage or Trojan insertion opportunities.
- **Formal Verification Extensions**: Integrating security checks (e.g., no untrusted backdoor paths, Trojan detection) into existing equivalence checking or property-based verification tools.
- **Co-Simulation of Thermal, Power, and Logical Dynamics**: A unified environment where designers can test how changes in the interconnect topology affect both performance and security across all layers.

E. Toward a Holistic Security Framework

Real-world 3D systems demand *layered defenses*—from front-end IP encryption to back-end side-channel mitigation. We must combine the following technologies:

- Reconfigurable routing,
- Chiplet authentication,
- Runtime monitoring and anomaly detection,
- Side-channel countermeasures,

into a cohesive framework can substantially reduce the chance of successful attacks on the interconnect. As these strategies mature, standardization efforts (e.g., security extensions to UCIe or CXL) may further encourage secure design practices industry-wide.

By pursuing these emergent directions, the research community can help ensure that the performance and flexibility gains of 3DICs do not overshadow the necessity of robust security. Rather, each layer—physical, architectural, and system-level—should be co-designed with security as a foundational requirement, laying the groundwork for trustworthy heterogeneous computing platforms.

VI. Conclusion and Future Work

Heterogeneous 3D integrated circuits have the potential to revolutionize system performance, scalability, and cost-effectiveness by stacking diverse chiplets—CPUs, GPUs, accelerators, and memory—in a compact form factor. Yet, this vertical integration and multi-vendor sourcing create new vulnerabilities that conventional 2D SoC security techniques cannot fully address. In particular, the 3D interconnect fabric, whether realized through TSVs or advanced interposer interfaces, emerges as a prime target for hardware Trojans, reverse engineering, and side-channel exploitation.

Throughout this paper, we have highlighted the unique threat landscape for 3D interconnects, ranging from supply-chain tampering to cross-tier side-channel attacks. We also introduced emergent research directions—such as dynamic obfuscation, chiplet authentication, and runtime monitoring—to mitigate these multidimensional risks. Taken together, these discussions affirm the urgency of designing holistic security solutions that tackle every phase of the 3DIC lifecycle, from fabrication to in-field operation.

Moving forward, *key opportunities* for innovation include:

- **Standardizing Security Extensions**: Collaborating on open standards (e.g., UCIe) that incorporate native authentication, encryption, and secure boot mechanisms for multi-chiplet 3D systems.
- **Combining Architecture-Level and Physical Defenses**: Layering reconfigurable obfuscation or protocol scrambling at the interconnect level with physical isolation techniques that reduce cross-tier side-channel leakage.
- **Automated EDA Toolchains**: Developing design flows that automatically account for stacked chiplet trust levels, routing complexity, and advanced testing (e.g., integrated Trojan detection), so engineers can enforce secure assembly at scale.

In essence, successful deployment of 3DICs will require a *concerted effort* to adapt and extend existing hardware security methods, as well as to innovate new strategies suited to layered architectures and heterogeneous integration. By embracing these research directions, the community can unlock the performance and economic advantages of 3D packaging without compromising the trustworthiness and reliability demanded by modern systems.

References

[1] 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.

[2] Y. Liu, D. Xing, I. McDaniel, O. Ozbay, A. Akib, M. I. Sukanya, S. Rekhi, and A. Srivastava, "Security advantages and challenges of 3d heterogeneous integration," *Computer*, vol. 57, no. 3, pp. 107–112, 2024.

[3] J. Suzano, F. Abouzeid, G. Di Natale, A. Philippe, and P. Roche, "On hardware security and trust for chiplet-based 2.5d and 3d ics: Challenges and innovations," *IEEE Access*, vol. 12, pp. 29 778–29 794, 2024.

[4] N. Vashistha, M. L. Rahman, M. S. U. Haque, A. Uddin, M. S. U. I. Sami, A. M. Shuo, P. Calzada, F. Farahmandi, N. Asadizanjani, F. Rahman, and M. Tehranipoor, "ToSHI - towards secure heterogeneous integration: Security risks, threat assessment, and assurance," Cryptology ePrint Archive, Paper 2022/984, 2022. [Online]. Available: https://eprint.iacr.org/2022/984

[5] D. Halder, M. Merugu, and S. Ray, "Obnocs: Protecting network-on-chip fabrics against reverse-engineering attacks," *ACM Trans. Embed. Comput. Syst.*, vol. 22, no. 5s, Sep. 2023. [Online]. Available: https://doi.org/10.1145/3609107

[6] D. Halder, Y. Liu, K. Amberiadis, A. Srivastava, and S. Ray, "Potent: Post-synthesis obfuscation for secure network-on-chip architectures," in *2024 IEEE 37th International System-on-Chip Conference (SOCC)*, 2024, pp. 1–6.

[7] Z. U. Abideen, S. Gokulanathan, M. J. Aljafar, and S. Pagliarini, "An overview of fpga-inspired obfuscation techniques," *ACM Comput. Surv.*, vol. 56, no. 12, Oct. 2024. [Online]. Available: https://doi.org/10.1145/3677118

[8] Z. U. Abideen and S. Pagliarini, *ReBO-Driven IC Design: Leveraging Reconfigurable Logic for Obfuscation*. Cham: Springer Nature Switzerland, 2025, pp. 43–56. [Online]. Available: https://doi.org/10.1007/978-3-031-77509-3_3