Physical Security Assessment of Advanced Packaging Structures

Liton Kumar Biswas *, Nitin Varshney *, Rouhan Noor *, Shajib Ghosh *,
Yashan Peng†, Jiaqi Tang†, and Navid Asadizanjani*
*University of Florida, Gainesville, FL, USA
†JIACO Instruments, Delft, Netherlands
Corresponding email: litonkumarbiswas@ufl.edu

2024 IEEE Physical Assurance and Inspection of Electronics (PAINE) | 979-8-3315-4225-2/24/$31.00 ©2024 IEEE | DOI: 10.1109/PAINE62042.2024.10792751

***Abstract*—The demand for System-in-Package (SiP) devices become more prevalent in various critical and industrial applications. As a result of this growing popularity, SiP devices are becoming more attractive to attackers who are seeking to exploit vulnerabilities. Chip security is one of the cornerstones of hardware security and has received considerable attention over the past two decades. With advances in SiP-enabled advanced packaging technology, a new concept called "security packaging of integrated circuits" has been developed to protect chips. This paper provides an in-depth analysis of SiP chip security packaging. In order to accomplish this, we explore MIP sample preparation technique in an effort to ensure that vulnerable locations can be accessed. Finally, by identifying potential vulnerable interfaces, we evaluate the effectiveness of existing security measures, ensuring protection and integrity of the SiP devices.**

***Index Terms*—Advanced packaging, heterogeneous integration, system-in-package (SiP), cryptographic keys, probing, security vulnerabilities.**

I. Introduction

The ubiquitous existence of electronic gadgets is significantly altering our lifestyle and occupation, getting intricately integrated into our everyday regimens. The extensive usage of fast gadgets and seamless communication in today's digitally driven economy generates a massive amount of data. To allow data-driven transactions, a number of vital technologies, including as data centers, artificial intelligence (AI) systems, and autonomous vehicles, depend on gathering, storing, and analyzing this massive amount of data. Integrated Circuits (ICs) are essential to the advancement of wireless communication, high-performance computing, and data processing. Modern ICs include high-speed input/output (I/O) ports, many computing cores, and high-bandwidth memory. Moore's Law is largely responsible for the existence of these state-of-the-art ICs, as it has continually pushed the semiconductor industry to manufacture ICs that are quicker, smaller, and more affordable.

A growing number of individuals have been doubting this law's continued reliability because of challenges with increasing transistor sizes (such as quantum phenomena) and rising production costs. As a result, cutting-edge tactics like Heterogeneous Integration (HI) have surfaced, fundamentally altering packaging and design methodologies and offering a fresh perspective on Moore's Law. These creative methods provide functional density greater weight as a performance indicator than transistor density alone, which opens up new avenues for the industry and yields insightful information and more precise forecasts. HI combines independently produced parts with different technological nodes and functions to create a more sophisticated assembly called a System-in-Package (SiP) or Multi-Chip Module (MCM). Improved operating features and expanded functionality are provided by SiPs, which are challenging to achieve with a single-die SoC method.

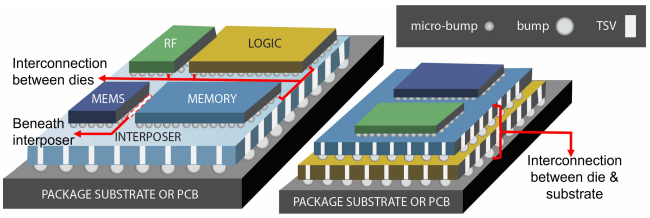

Fig. 1. Heterogeneous Integration in a system-in-package of 2.5D and 3D IC packages with interposers, bumps, micro-bumps, and through-silicon vias, and focuses potential the vulnerable locations [6].

The SiP may include several pieces, including chiplets, active/passive components, and MEMS devices, into a single, cohesive package as shown in Fig. 1. The advancement of HI solutions is heavily influenced by a number of significant participants in the semiconductor industry, including integrated device manufacturers (IDM) like Intel, Micron, and Samsung, fabless design companies like AMD and IBM, foundries like TSMC and Samsung, and OSATs like Amkor and TSMC. Examples of 3D SiPs that are commercially available include AMD EPYC and Intel Lakefield processors [1]. A similar goal is shared by the Defense Advanced Research Projects Agency (DARPA) and its Common HI and Intellectual property (IP) Reuse Strategies (CHIPS) Program, which aims to advance reliable microelectronics for the US Department of Defense's (DoD) applications and technological requirements [2], [3]. As of 2023, the global SiP market is valued at approximately $33.9 billion and is projected to reach $58 billion by 2030,

growing at a compound annual growth rate (CAGR) of 8%. The Asia-Pacific region, particularly China, dominates the market due to its large-scale manufacturing capabilities and significant demand from the consumer electronics sector.

A crucial component of cybersecurity is hardware security, which covers a variety of possible risks and weaknesses related to a system's physical components. Security flaws can still be introduced by the design and manufacturing processes, even if the supply chain is entirely within the US and well-protected. Rogue workers and other malicious actors may try to introduce backdoors, Hardware Trojans (HT) [4], [5], or other harmful elements at any step of the production process or across the supply chain. Reverse Engineering (RE) is another big issue that never goes away, even after the US-based semiconductor supply chain is completely safe and comes onshore. Chiplets include reprocessing and photographing different device layers from produced ICs in order to retrieve design data at the register-transfer level (RTL) level. RE can provide rival semiconductor design firms or advertising foundries a financial and competitive advantage.

Sample preparation, or S-prep, is crucial to semiconductor devices because it helps remove elements that aren't needed for hardware assurance and failure analysis (FA) [7]. However, prior research has frequently undervalued the importance of S-prep. Internal imperfections in these chips may be found by using S-prep, which makes a variety of inspections and probing investigations easier. These techniques are critical for failure site diagnosis in FA and support inspection techniques including materials analysis, nano-probing, transmission electron microscopy (TEM), and scanning electron microscopy (SEM). These techniques may also be used to find hardware security vulnerabilities in semiconductor devices. This paper offers an in-depth look at S-prep in the realm of complex HI packaging, emphasizing the necessity of precise methodologies like atmospheric microwave-induced plasma (MIP) and thorough structural analysis for effective and efficient sample preparation. Though conventional plasma etching is suitable for uniform etching during batch wafer fabrication, not enough for package decapsulation. It has to be localized plasma to remove EMC. To remove EMC with enhancing the etching rate, MIP can be employed. This approach involves pure chemical etching using neutral atomic oxygen radicals, which reduces potential damage from ion bombardment and stress to silicon die. Therefore, MIP is more efficient to analyze security vulnerabilities, keeping the device functionality intact.

This paper is organized as follows: Section II provides the information on the background for advanced packaging technologies and their possible vulnerable interfaces. It also provides background for various sample preparation techniques. Section III introduces the workflow and the challenges for our proposed sample preparation technique. Section IV discuss about the experimental setup and the results for security analysis of advanced packaging. Section V provides a future direction for this research. Finally, section VI concludes the paper.

II. Background

A. Advanced packaging technologies

1) 2.5-D packaging: An interposer layer is used between chiplets and the packaging substrate to create 2.5-D packages. These devices are typically connected by high-speed data buses through an interposer. A 2.5-D packaging method that uses TSVs is Chip-on-Wafer-on-Substrate (CoWoS), a method that stacks multiple chiplets on silicon interposers [8] (Refer in Fig. 1). Interposers are mounted onto substrates using flip-chip or wire bonding technologies, and they contain Redistribution Layers (RDLs) that redistribute signals. In this method, different chiplets can be integrated, such as memory, processors, and sensors. Different interposer materials have been developed by companies such as IBM, TSMC, and ASE for 2.5-D packaging.

In addition to 2.5-D packaging methods, it is also possible to connect adjacent chips using bridges. Embedded Multi-Die Interconnect Bridges (EMIBs) are embedded in packaging substrates after being fabricated separately [9]. Interconnecting chiplets using this method is sometimes referred to as 2.3-D packaging. The cost-effectiveness of bridge solutions over interposer-based 2.5-D packaging is driving the development of bridge solutions.

2) 3-D packaging: Through silicon vias (TSVs) connect three-dimensionally stacked semiconductor dies. Memory can be stacked on processors using this technology, or analog and digital circuits can be integrated using this technology. A great example is Intel's Foveros, which stacks different functional dies with TSVs and microbumps to provide electrical connectivity [10] (Refer in Fig. 1). Three-dimensional packaging is also used in imaging sensors and portable devices, such as Package-on-Package (PoP), which connects two packaged dies vertically by using package vias (TPVs).

3) Co-packaged optics (CPOs): At every step, semiconductor packaging roadmaps emphasize robust interfaces, but determining the best interface for a particular application can be difficult due to the many possible options. Emerging processes like wafer-to-wafer bonding, backside power distribution, and co-packaging optics, which integrate optical and electronic components, in the same package, enhance performance, power efficiency, and thermal management by reducing interconnects. As an example, co-packaged optics might entail placing the optical components on the same silicon interposer used in 2.5D packaging enabling high-speed data communication. As a global leader in CPO solutions, Broadcom serves high-growth markets including networking, AI/ML, and high perfomance computing (HPC) [11]. CPOs are developed by Intel that can be replaced with plug-and-play assemblies, ensuring high-performance systems with greater functionality.

B. Vulnerable interfaces of advanced packaging

1) Die to Die interface: The die-to-die interface in advanced packaging (refer in Fig. 2), especially within SiP and 3D integrated circuits, is susceptible to security vulnerabilities

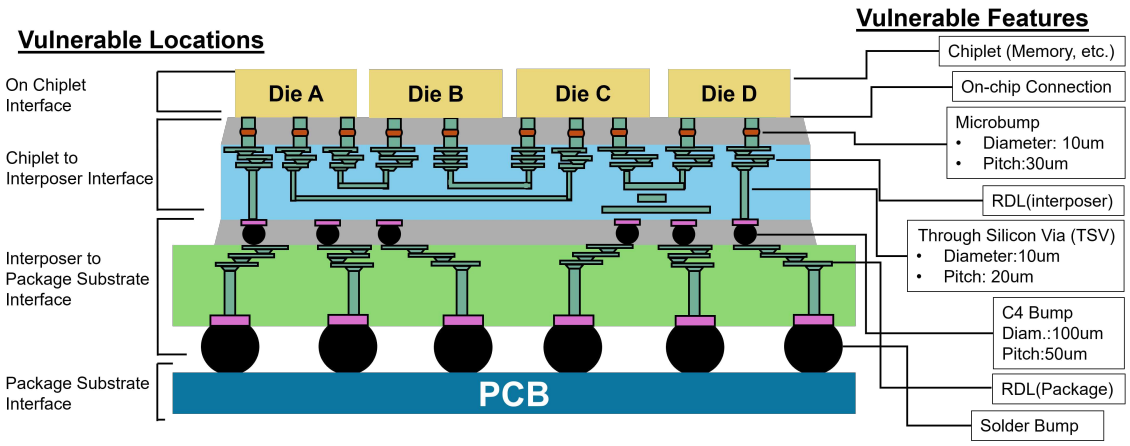

Fig. 2. Potential vulnerable locations and features in advanced packaging

due to the dense interconnections required for high-speed data transfer. This interface facilitates communication between different functional units of the package, such as processors and memory units [12]. High-density interconnects, often in the form of microbumps, are used to achieve this communication. Probing attacks like nanoprobing can exploit these microbumps to tap into the signal pathways between dies, potentially intercepting sensitive information. For instance, if an encryption key is being transferred from one die to another, an attacker could use a fine-tipped probe to access the signal and capture the key.

2) Die to interposer interface: The interface between the die and the interposer is another critical point of vulnerability as shown in Fig. 2. This interface typically involves microbumps and redistribution layers (RDLs), providing electrical connectivity between the die and the interposer [13]. Probing attacks, such as electron beam (E-beam) probing or focused ion beam (FIB)/SEM nanoprobing, can target these microbumps and RDLs to access internal signals. Effective sample preparation techniques, such as precise deprocessing and backside thinning, expose these interfaces for probing, making them vulnerable to sophisticated attacks. For example, an attacker could prepare a sample by thinning the backside of the die to expose the microbumps and then use E-beam probing to monitor and extract data being transferred through the die-to-interposer connections.

3) Interposer to package substrate interface: The connection between the interposer and the package substrate is crucial for signal integrity and overall package functionality. This interface typically comprises solder bumps or other high-density interconnects that connect the interposer to the substrate [14]. Vulnerabilities at this interface can be exploited using physical inspection techniques, such as X-ray imaging or acoustic microscopy, to reveal internal structures. Once exposed, these interconnects can be probed to extract data or disrupt signal paths. An attacker could use X-ray imaging to locate the solder bumps and then employ a probe to tap into the interconnects, capturing sensitive data packets traveling between the interposer and the package substrate.

4) Package substarte interface : The interface between the package substrate and the external environment is a critical boundary for the security of the entire package. This interface often includes exposed connections such as solder balls and C4 bumps that physical attacks can target. Probing these connections can provide attackers access to the internal circuitry and data paths. To defend against such attacks, advanced packaging techniques must incorporate protective layers and shielding materials. Additionally, anti-tamper technologies and continuous monitoring of package integrity can help mitigate the risks associated with vulnerabilities at the package substrate interface. For example, an attacker might use physical probing to tap into the C4 bumps, extracting sensitive data such as cryptographic keys being transferred through the package substrate.

An example of a probing attack could involve an attacker targeting a sensitive node within the die-to-die interface. Suppose there is a node that carries cryptographic keys used for securing communications between two dies. An attacker could use nanoprobing to locate this node and place a probe on the precise interconnects (RDL) in the interposer. By intercepting the signals at this node, the attacker could capture the transferred cryptographic keys, compromising the system's security. This intercepted key could then be used to decrypt confidential communications, leading to significant data breaches and loss of sensitive information.

C. Sample preparation for advanced packaging

To investigate the vulnerabilities of the advanced packaging, device under test (DUT) needs to be prepared with desired level of precision. This involves several critical steps. In decapsulation, the external protective covering of an IC is removed to reveal the internal circuitry, which can then be analyzed, tested, or modified. This process can be done in different techniques including wet etching, dry etching.

Wet etching plays an essential role in the preparation of samples for analysis and characterization in addition to

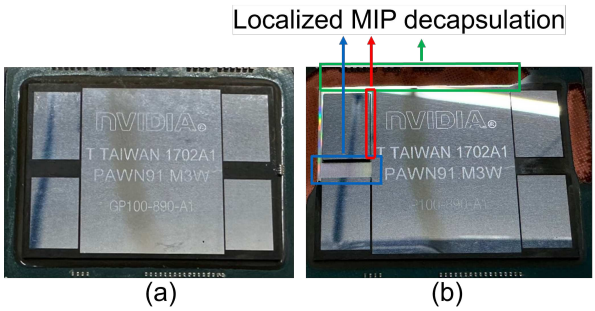

Fig. 3. Overview images of the 2.5D module (a) before and (b) after localized MIP decapsulation.

semiconductor device fabrication. Wet etching is an isotropic etching that can lead to undercutting, therefore it is challenging to keep uniform [16]. The removal of material from a micro-machining process (cutting) should be directional for precision micro-machining. Isotropic wet etches typically etch faster, however, isotropic wet etches are not capable of making features with higher aspect ratios [17].

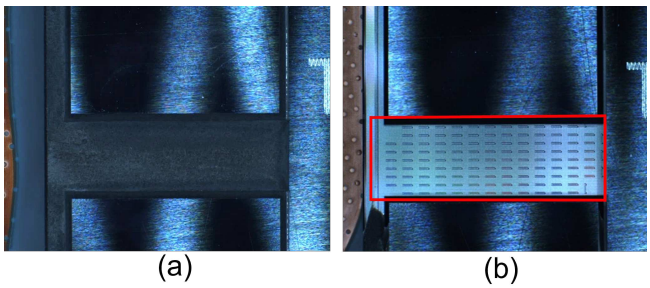

Fig. 4. Images of the 2.5D module (a) before and (b) after localized MIP decapsulation.

Therefore, it is possible to control the endpoint precisely when using dry etching. Dry etching can be achieved using lasers and plasma. Mold compound can be delayered using a standard laser ablation tool. A major advantage of laser ablation is the ability to control and precisely remove material. Laser ablation is very useful until far away from the circuitry. The plasma etching process is suitable for a variety of semiconductor materials, including silicon, silicon dioxide, silicon nitride, as well as metals [18]. Due to its versatility, it is suitable for preparing semiconductor samples at various stages of the manufacturing process. In addition, when high aspect ratio or small feature devices need high anisotropy, dry etching with plasma is the most commonly used. In addition to providing a degree of control, plasma etching can be tailored to provide a highly anisotropic result, although it is more challenging to achieve excellent selectivity with the procedure.

III. DUT Preparation and Challenges

A. Workflow of the sample preparation

The Epoxy Molding Compounds (EMCs) in advanced packages protect the dies from environmental factors and ensure the top surfaces of the dies are planarized [19], [20]. However, EMCs also limit access to embedded components, making analyzing advanced package modules more challenging. Accurate fault isolation and failure mode identification necessitate the removal of EMCs without damaging die surfaces, interfaces, and structures. Conventional acid decapsulation is a relatively fast method to remove EMCs. However, acid often corrodes the micro bumps, bond pads, and printed circuit board (PCB) substrate, which complicates subsequent failure analysis or structural analysis.

In this paper, atmospheric microwave-induced plasma (MIP) is used to remove EMCs and underfill, thereby exposing various die surfaces on the 2.5D package. Unlike conventional vacuum-based plasma etchers designed for large-area etching, MIP employs a localized etching technique with a focused plasma beam. Moreover, MIP demonstrates an etching rate at least ten times higher than vacuum-based plasma etchers because of its superior radical flux [19]. The MIP etching process does not involve ions as reactants, so it does not cause charging or ion bombardment damage. As a result, the electrical functionality and data in the die remain intact after MIP decapsulation. These capabilities make MIP particularly suitable for advanced 2.5D and 3D package sample preparation.

In the MIP system, plasma is generated within a discharge tube inside a Beenakker cavity with oxygen as the etchant gas. The plasma effluent, which carries atomic oxygen radicals, is then directed downwards to the selected area for etching. Oxygen plasma selectively removes organic materials from EMCs and leaves behind inorganic fillers on the surfaces. To remove the fillers, an automatic ultrasonic cleaning process is integrated into the MIP process. Consequently, the sample undergoes multiple etch-clean cycles to expose the required areas.

As shown in Figures 3, 4, and 5, the areas of interest in the 2.5D package module were fully exposed by the MIP process, and even the EMC in the gap between the HBM and graphics processing unit (GPU) dies was removed, revealing the underlying interposer die. No damage was introduced during MIP decapsulation.

B. Challenges of the sample preparation

Microbumps under chiplets are challenging to expose without causing damage due to their positioning. FIB milling is commonly used to access microbumps. Cross-sectioning, despite offering detailed insights into the internal structures, is inherently destructive as it involves cutting through the package module. MIP presents a potential alternative for removing underfill and exposing microbumps between the stacked dies by undercut etching. However, the etching depth depends on plasma gas penetration between the top dies and the interposer die. In this sample, the narrow gap between HBM or GPU and the interposer die does not allow sufficient plasma gas for undercut etching, therefore limiting the exposure of the microbumps.

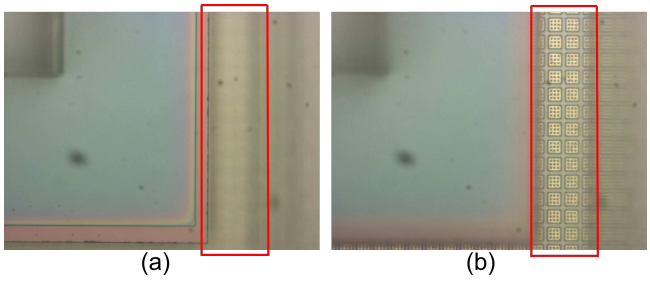

Fig. 5. Optical images of (a) the base die surface and (b) the interposer die surface between HBM and GPU after MIP decapsulation.

IV. Security Analysis of Advanced Packaging

A. Sample description

An Nvidia Tesla P100 GPU is selected as the example, which employs the Chip-on-Wafer-on-Substrate (CoWoS) method for high-performance computing. As part of this heterogeneous system, a GPU die made by TSMC is integrated with a High Bandwidth Memory 2 (HBM2) stack made by Samsung using a 16-nm process. Both are mounted on a 3500-mm² interposer die.

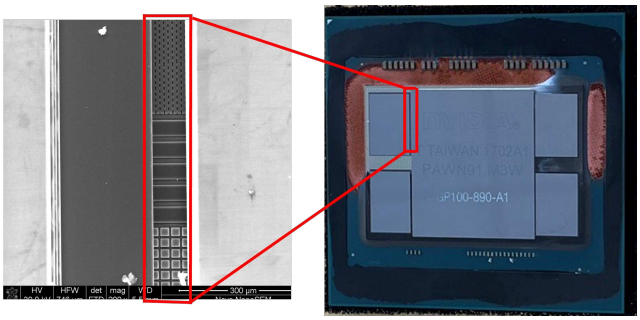

Fig. 6. Optical images of whole package and SEM Imaging of narrow gap between HBM and GPU

B. Vulnerabilities analysis

As far as security implications are concerned, it is important to note that the interposer layer can be a potential vulnerability. A thorough examination of the interface between the interposer layer and the chiplets can provide security researchers and adversaries alike with valuable information regarding the chip's internal workings. Accessing and interacting with the interface layer typically involves precise physical probing techniques. In order to extract information from the interposer layer, one needs to prepare a sample, expose the sensitive area, and then probe it with the help of a nanoprobing. As a result, it becomes possible to monitor the data transmission between chiplets. One of the area of interests indicates narrow gap between GPU and HBM as shown in Fig. 6. The interface between GPU and HBM might communicate through the interposer. After taking sample preparion, SEM imaging shows distinct patterns at that area of interest.

A precise sample preparation technique determine how much exposure lies beneath the chiplets. The localized MIP etching process, as depicted in the images (refer in Fig. 6), shows effective removal of EMCs and exposure of the interposer die. However, full exposure of the microbumps and interposer connections is challenging due to the narrow gaps and protective materials that shield these components. While MIP etching provides a non-destructive means to access certain areas, achieving complete exposure without damage requires advanced techniques like FIB milling, which can precisely remove materials but is inherently destructive. Thus, the degree of exposure is limited by the available technology and the need to balance accessibility with the preservation of the sample's integrity.

Limited access to the interposer layer interfaces presents significant challenges in both probing and analysis. The primary barrier is the protective EMCs and the lateral and vertical narrow gaps of between stacked dies which restrict the penetration of probing tools. Conventional methods like acid decapsulation are unsuitable as they can corrode essential components, complicating further analysis. MIP etching offers a promising alternative, providing non-destructive exposure of critical areas without ion bombardment damage. However, its effectiveness is limited by the depth of plasma gas penetration, especially in tight spaces. FIB milling, while offering detailed access, is destructive and can damage the sample. These limitations necessitate a combination of techniques to balance thorough examination with minimal damage, posing a significant challenge to researchers and security analysts.

Vulnerable locations that can be exposed without damaging the samples include the regions between the HBM and GPU and HBM where MIP etching effectively removes EMCs. These areas, visible in the optical and SEM images, offer access to the interposer die's surface and the RDLs without causing damage as shown in Fig. 7. The precise, non-destructive nature of MIP etching allows for selective removal of protective materials, exposing critical points for potential probing. However, complete exposure to microbumps or any interconnects inside the interposer remains challenging without more invasive techniques. Fig. 7 shows SEM imaging of different locations between HBM and GPU or HBM with different features, however it needs to remove more materials in the interposer to get access the vulnerable points. Fig. 7 (c) and (d) indicate the subsurface image which might have possibility of interconnects. The goal is to identify and target regions where sufficient access can be achieved with minimal impact on the sample's structural integrity, allowing for effective security analysis while preserving the component's functionality.

Accessing the interposer layer exposes several security vulnerabilities:

1) Data interception: Sensitive information, such as cryptographic keys, can be intercepted during transmission between chiplets. This is particularly concerning in high-security environments where data integrity and confidentiality are paramount.

2) Communication manipulation: An attacker could alter the data being transmitted, leading to misinformation or ma-

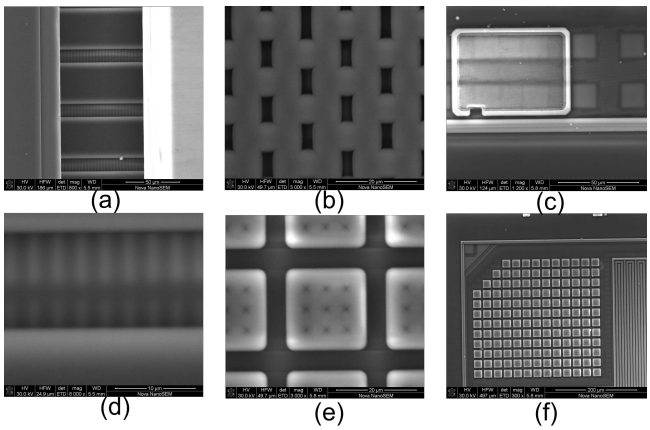

Fig. 7. SEM imaging of the interposer layer around and between HBM and GPU at different location from (a) to (f)

licious instructions being executed by the chiplets. This could disrupt normal operations and introduce faults into the system.

3) Introduction of malicious modifications: Unauthorized modifications at the hardware level can compromise the entire system's integrity. These modifications can lead to hardware-level vulnerabilities that are difficult to detect and mitigate, potentially allowing long-term exploitation.

4) Hardware-level vulnerabilities: Physical access to the interposer layer can enable attackers to introduce backdoors or other malicious hardware components, creating persistent vulnerabilities that software-level security measures cannot address.

The challenges in addressing these vulnerabilities include the difficulty in detecting such sophisticated attacks and the technical limitations of non-destructive probing methods. Advanced protective measures, continuous monitoring of package integrity, and robust anti-tamper technologies are essential to safeguard against these potential threats. Developing and implementing these defenses requires ongoing research and innovation to stay ahead of evolving attack methodologies.

This extended analysis highlights the critical security concerns associated with the interposer layer, emphasizing the need for meticulous examination and innovative protective strategies to mitigate the risks posed by potential adversaries.

V. Future Direction

This study emphasizes the value of S-prep in the field of hardware assurance (HW), particularly in light of the rise of HI packaging, which combines chiplets and interposers in a stack. This restricts the application of current non-destructive physical examination methods and emphasizes the significance of exposing the target region with S-prep. However, there have also been some noted challenges while employing MIP for HI packaging.

Future research directions encompass several key areas:

- Localization and focusing on areas that can be adequately accessed with minimal influence on the sample's structural integrity, enabling efficient security analysis without compromising the component's performance.
- A significant avenue for future research involves performing the sample preparation on commercial SiP while keeping the chip electrically active and further using capabilities like Nano-probing and E-beam probing to probe those vulnerable areas between chiplets in a HI packaged chip. This expansion aims to explore the security vulnerabilities of SiPs.

VI. Conclusion

The increasing popularity of SiPs poses significant security challenges, facilitated by probing techniques. A part of the discussion in this article was devoted to addressing these challenges in the context of SiPs. Emphasis was placed upon the vulnerability of the internal structure especially the interconnection of advanced packaging, which is responsible for routing signals between chiplets. Another part of our discussion, we explored the workflow of the atmospheric MIP to prepare the sample along with challenges to expose potential vulnerability for testing. By combining MIP and SEM, we were able to demonstrate the vulnerable interface in advanced packaging without causing any damage to it.

Acknowledgment

The author would like to extend thanks to JIACO Instruments group for their invaluable support and collaboration, and Sai Pranesh Amirisetti from ECE UF for his assistance in this work.

References

[1] P. A. l. updated. "AMD announces x3d chip stacking and infinity architecture," Tom's Hardware. (Mar. 5, 2020), [Online]. Available: https://www.tomshardware. com/news/amd- announces - x3d- chip-stacking- and- infinity-architecture.

[2] S. Ravi. "CHIPS for america act & FABS act," Semiconductor Industry Association. Available: https://www.semiconductors.org/ chips

[3] "CHIPS.gov," NIST, May 11, 2022, Last Modified: 2023-06-23T06:18-04:00

[4] Varshney, Nitin, Haoting Shen, Olivia Paradis, and Navid Asadizanjani. "He-ion beam imaging for accurate hardware Trojan detection." Microscopy and Microanalysis 26, no. S2 (2020): 188-190.

[5] Tehranipoor, M. M., Asadi-Zanjani, N., Paradis, O. P., & Varshney, N. (2023). U.S. Patent No. 11,604,912. Washington, DC: U.S. Patent and Trademark Office.

[6] Metrology capabilities keep up with semiconductor industry push into 3d integrated circuits (part 1) - 2024 - wiley analytical science," Analytical Science Article DO Series. (), [Online]. Available: https : / / analyticalscience . wiley . com / do / 10 . 1002

[7] F. Altmann and M. Petzold, "Innovative failure analysis techniques for 3-d packaging developments," IEEE Design & Test, vol. 33, no. 3, pp. 46–55, 2016.

[8] S. Y. Hou et al., "Wafer-level integration of an advanced logic-memory system through the second-generation CoWoS technology," IEEE Trans. Electron Devices, vol. 64, no. 10, pp. 4071–4077, Oct. 2017.

[9] R. Mahajan et al., "Embedded multi-die interconnect bridge (EMIB)—A high density, high bandwidth packaging interconnect," in Proc. IEEE 66th Electron. Compon. Technol. Conf. (ECTC), May 2016, pp. 557–565.

[10] D. B. Ingerly et al., "Foveros: 3D integration and the use of face-to-face chip stacking for logic devices," in IEDM Tech. Dig., Dec. 2019, p. 19.

[11] "Broadcom CPO: Highest power efficiency and band-width density." Available: https : / / www.broadcom.com/info/optics/cpo.

[12] Biswas, Liton Kumar, et al. "Emerging nonvolatile memories—an assessment of vulnerability to probing attacks." International Symposium for Testing and Failure Analysis. Vol. 84437. ASM International, 2022.
[13] Khan, M. Shafkat M., et al. "Secure interposer-based heterogeneous integration." IEEE Design & Test 39.6 (2022): 156-164.
[14] Khan, Aslam A., et al. "Security Assessment of Interposer in Advanced Packaging."
[15] W.-C. Chen et al., "Development of novel fine line 2.1 D package with organic interposer using advanced substrate-based process," in Proc. IEEE 68th Electron. Compon. Technol. Conf. (ECTC), May 2018, pp. 601–606.
[16] https://resources.pcb.cadence.com/blog/2024-wet-etching-vs-dry-etching.
[17] https://www.wevolver.com/article/dry-etching-vs-wet-etching.
[18] Lin, Yuanwei. "Perspective on Plasma Etching in Advanced Packaging." 2024 Conference of Science and Technology for Integrated Circuits (CSTIC). IEEE, 2024.
[19] Hong Siang Tan, B. Zee, Chee Lip Gan, K. Kor, J. Tang, and M. McKinnon, "Oxygen-Based Microwave Induced Plasma Etching for Epoxy Molding Compound Removal in Advanced Semiconductor Devices," Jul. 2023.
[20] "November edfa digital." Section: Article Section. (), [Online]. Available: https://static.asminternational.org/ edfa/202111/14/.