Securing Heterogeneous 2.5D ICs Against IP Theft through Dynamic Interposer Obfuscation*

Jonti Talukdar*, Arjun Chaudhuri*, Jinwoo Kim†, Sung Kyu Lim†, and Krishnendu Chakrabarty*
*Department of Electrical and Computer Engineering, Duke University, Durham, NC
†School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA

***Abstract*—Recent breakthroughs in heterogeneous integration (HI) technologies using 2.5D and 3D ICs have been key to advances in the semiconductor industry. However, heterogeneous integration has also led to several sources of distrust due to the use of third-party IP, testing, and fabrication facilities in the design and manufacturing process. Recent work on 2.5D IC security has only focused on attacks that can be mounted through rogue chiplets integrated in the design. Thus, existing solutions implement inter-chiplet communication protocols that prevent unauthorized data modification and interruption in a 2.5D system. However, none of the existing solutions offer inherent security against IP theft. We develop a comprehensive threat model for 2.5D systems indicating that such systems remain vulnerable to IP theft. We present a method that prevents IP theft by obfuscating the connectivity of chiplets on the interposer using reconfigurable interconnection networks. We also evaluate the PPA impact and security offered by our proposed scheme.**

I. Introduction

The globalization of the integrated circuit (IC) supply chain poses significant risk to the security of intellectual property (IP). Of particular concern is the vulnerability to IP theft through attacks such as netlist reverse-engineering, counterfeiting, and IC overbuilding. Security challenges associated with the integration of chiplets on an interposer can lead to threats arising from within the system, for example, through rogue or untrusted chiplets as well as threats arising from outside the system, e.g., through an untrusted end-user [1]. In this work, we explore the security challenges arising from the integration of chiplets on an interposer (2.5D ICs) by formulating a strong threat model. A key shortcoming of existing 2.5D security solutions [2] is the assumption of a secure runtime environment during functional operation, which limits the scope of existing protection schemes to threats arising from within the system, e.g., hardware Trojans, rogue chiplets, etc. We describe a more comprehensive threat model that considers the relevant attack surfaces applicable for a heterogeneously integrated 2.5D system. We next propose a security solution that aims to obfuscate the interconnections between chiplets on the interposer using a reconfigurable interconnection network, referred to as a *scrambler*. We evaluate the security benefits of the scrambler. The key contributions of this work are as follows: (1) Expanding the threat model applicable for 2.5D ICs, covering invasive and non-invasive attacks. (2) Developing a novel interconnect obfuscation method for 2.5D ICs based on reconfigurable interconnection networks. (3) Evaluating the security and PPA impact of the proposed solution.

*This research was supported in part by the Semiconductor Research Corporation (Task ID 2994.001) and the NSF under grant no. CNS-2011561.

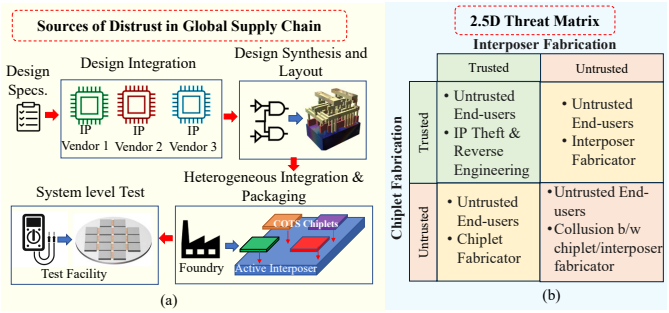

Fig. 1: (a) Sources of distrust in globalized supply chain (b) Threat matrix for 2.5D HI systems.

The rest of the paper is organized as follows. Section II reviews the 2.5D HI threat model. Section III presents the interconnect scrambler design with Section IV reviewing its PPA impact. Section V concludes the paper.

II. Threat Modeling for 2.5D HI Systems

A. Heterogeneous Integration: Security Threats

Threats in 2.5D ICs can be categorized based on their source: *(1) Rogue or Untrusted Chiplets:* An untrusted chiplet with rogue IP may exercise unauthenticated functions, snoop data, and mount various attacks through the shared interconnects implemented on the interposer. *(2) Untrusted End-Users:* Stealing IP integrated in the 2.5D system is the most prominent threat posed by an untrusted end user because they may try to exploit both physical and scan-based side channels as well as traditional approaches such as netlist reverse engineering (RE) to achieve their objectives. Existing 2.5D root-of-trust (RoT)-based solutions focus on protection against malicious modifications or system level threats arising from untrusted chiplets through enforcement of security policies for memory access integrity during runtime [2], [3]. However, these methods fail to consider attacks mounted through external environment, including IP theft from untrusted end users.

B. Threat Modeling for 2.5D ICs

We can segregate the parties involved in heterogeneous 2.5D integration into two categories, the chiplet manufacturer and the interposer manufacturer. Either all the chiplets in the design could be sourced from a trusted source, or a certain number of chiplets could be sourced from an untrusted source. As multiple manufacturers can be sourced to procure chiplets in the system, we assume that a certain number of chiplets in the design are untrusted for a general use case. Similarly, the interposer could be fabricated either in an untrusted or trusted environment. The above scenarios lead to the threat matrix presented in Fig. 1(b).

978-3-9819263-7-8/DATE23/© 2023 EDAA

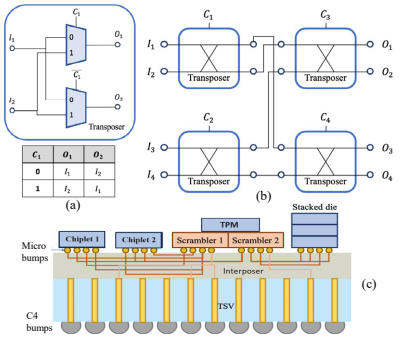

Fig. 2: (a) 2×2 Transposer architecture with truth table. (b) A 4×4 non-blocking interconnect scrambler, (c) Scrambler on 2.5D interposer.

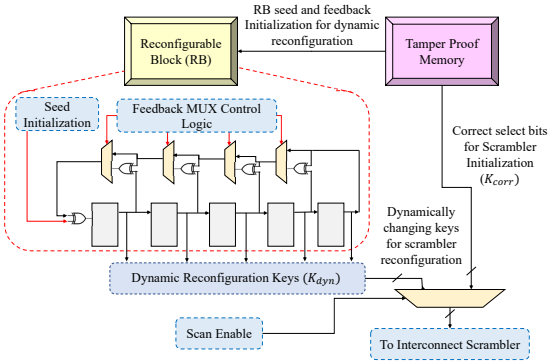

Fig. 3: Integrating RBs for enabling dynamic scrambler reconfiguration to prevent functional access to the Oracle.

III. Dynamic Interconnect Obfuscation

A. Interconnect Scrambler Design and Architecture

To prevent IP theft through interposer reverse engineering, we utilize interconnect scramblers that structurally obfuscate the chiplet-to-chiplet and chiplet-to-TSV connections on the interposer. The interconnect scrambler is designed as a cascaded network of an individual 2×2 switching blocks called the transposer. As illustrated in Fig. 2(a), a transposer consists of a pair of key controlled multiplexers that can reroute the incoming signals (I_1, I_2) across the output signals (O_1, O_2) depending on the value of the supplied key C_1. This 2×2 transposer serves as the building block for the interconnect scrambler. The scrambler has equal number of input and output signals (N), thereby making it a rectangular multi-stage interconnection network [4]. A non-blocking interconnection architecture is adopted that can be generalized for an $N \times N$ interconnect network where the number of intermediate stages supported by a 2×2 transposer is given by $\log_2 N - 2$. As a result, such a design requires $O(N \log_2 N)$ transposers. As illustrated in Fig. 3, the scrambler control bits (K_{scr}) are initialized with the correct keys (K_{corr}) from the tamper-proof memory. Dynamic obfuscation is achieved upon scan access by generating dynamic keys from LFSR-based reconfigurable blocks, such that $K_{scr} = K_{dyn}$ [5]. This ensures dysfunctional oracle access, preventing any form of oracle-guided attack [6].

B. Security Analysis

An attacker can attempt to guess the control values of all the transposers within the scrambler. As a single N scrambler will have at least $N \log_2 N$ transposers, the overall brute force attack effort is quantified as $2^{N \log_2 N}$. An attacker can also mount a removal/reconstruction attack where they remove the scrambler altogether and aim at reconstructing the functional connectivity between chiplets that now remain unconnected. In such a scenario, the reconstruction effort can then be quantified by the number of possible ways in which the open connections can be re-wired. For an $N \times N$ scrambler, the total number of possible connections between the input and the output is N!.

TABLE I: PPA overhead for scrambler-inserted on passive interposer.

Benchmark	Scrambler Arch.	Area (%)	Power (%)	Δ_{WL} (%)	t_{crit} (ns)
Cascaded FIR	8×8	39.5	0.69	11.75	1.82
	16×16	50	1.24	16.53	1.82
Cascaded IIR	8×8	39.5	0.24	8.42	1.81
	16×16	50	0.44	11.35	1.81
Triple DES	8×8	0	2.02	142.32	1.79
	16×16	0	2.94	152.1	1.79

IV. Overhead Analysis

Table I summarizes the PPA overhead for different scrambler sizes across multiple passive interposer-based 2.5D use-cases developed using IPs from the common evaluation platform (CEP) [7]. We use cascaded DSP IPs (FIR, IIR filters) and a crypto IP (triple-DES) for 2.5D integration. The system-level RTL including the scrambler is synthesized using Synopsys DC. The different chiplet IPs could be either black-boxed or designed in house. The chiplets are then passed through the floorplanning stage followed by micro-bump assignment, place, and route; all done using Cadence Innovus. All designs are based on the Nangate-45nm PDK. The μ-bump pitch considered for active and passive 2.5D interposer chiplets is $20\mu m$. The bottom six metal layers of the Nangate back-end-of-line (BEOL) stack are used for intra-chiplet routing to create hard chiplet macros. This is followed by the routing of the hard chiplet macros via the interposer using the top four metal layers of Nangate BEOL. The chiplet μ-bump arrays are placed placed on metal-7 $(M7)$ as pin constraints for the interposer routing. All systems are designed with target $t_{crit} = 2$ ns. Scrambler insertion does not impact the system's f_{max}.

V. Conclusion

We have presented the shortcomings of existing security solutions for 2.5D systems. We have described a method to secure the interconnections through the 2.5D interposer using interconnection scramblers. We have evaluated the security and overhead of the associated method, demonstrating that security is enhanced with low overhead.

References

[1] "Heterogeneous Integration Roadmap: Security," *IEEE EPS*, 2021.
[2] M. Nabeel et al., "2.5 D root of trust: Secure system-level integration of untrusted chiplets," *IEEE Trans. on Comp.*, vol. 69, no. 11.
[3] H. Park et al., "Design Flow for Active Interposer-Based 2.5-D ICs and Study of RISC-V Architecture With Secure NoC," *IEEE Trans. on Comp., Packaging and Manuf. Tech.*, vol. 10, no. 12.
[4] D.-J. Shyy et al., "Log/sub 2/(N, m, p) strictly nonblocking networks," *IEEE Trans. on Comm.*, vol. 39, no. 10, pp. 1502–1510, 1991.
[5] J. Talukdar et al., "A BIST-based Dynamic Obfuscation Scheme for Resilience against Removal and Oracle-guided Attacks," in *ITC 2021*.
[6] ——, "TaintLock: Preventing IP Theft through Lightweight Dynamic Scan Encryption using Taint Bits," in *IEEE ETS 2022*.
[7] B. Tan et al., "Benchmarking at the frontier of hardware security: lessons from logic locking," *arXiv:2006.06806*, 2020.