Security Threats and Countermeasures in Three-Dimensional Integrated Circuits

Jaya Dofe[1], Peng Gu[2],
[1]Department of Electrical and Computer Engineering
University of New Hampshire
qiaoyan.yu@unh.edu

Dylan Stow,[2]Qiaoyan Yu[1],
[2]Department of Electrical and Computer Engineering
University of California
yuanxie@ece.ucsb.edu

Eren Kursun[3], Yuan Xie[2]
[3]Department of Computer Science
Columbia University
ek2925@columbia.edu

ABSTRACT

Existing works on Three-dimensional (3D) hardware security focus on leveraging the unique 3D characteristics to address the supply chain attacks that exist in 2D design. However, 3D ICs introduce specific and unexplored challenges as well as new opportunities for managing hardware security. In this paper, we analyze new security threats unique to 3D ICs. The corresponding attack models are summarized for future research. Furthermore, existing representative countermeasures, including split manufacturing, camouflaging, transistor locking, techniques against thermal signal based side-channel attacks, and network-on-chip based shielding plane (NoCSIP) for different hardware threats are reviewed and categorized. Moreover, preliminary countermeasures are proposed to thwart TSV-based hardware Trojan insertion attacks.

1. INTRODUCTION

Three-dimensional (3D) integration is an emerging technology to ensure the growth in transistor density and performance that is expected for future integrated circuits (ICs) [1, 2]. It has been demonstrated that 3D techniques can be leveraged to reduce package size and power consumption while significantly improving bandwidth. However, 3D integration technology is a double-edged sword, as it introduces unique and unexplored challenges on managing related security issues.

1.1 History and Benefits of 3D IC

The growth of the semiconductor industry has long relied on the continual trend of increasing integration. As interconnect and transistor scaling both decelerate, the industry must look for alternate growth opportunities. 3D integration and similar forms of die-level integration provide novel design methodologies to increase transistor density, reduce interconnect distances, and integrate additional system components. 3D integration covers a range of different technologies, from interposer-based 2.5D methodology to monolithic sequential integration, but 3D stacked die-level integration, based on microbumps and Through-Silicon Vias (TSV), is widely seen as one of the most promising technologies for meeting future needs [3]. In this methodology, separate dies are fabricated using standard lithography, TSVs are added (during or after lithography), individual dies or wafers are thinned, and 3D stacks are formed through alignment and bonding. Over the last two decades, many improvements have been made in the process technology, design automation, and system architecture for these 3D circuits [4, 5]. Die-die interconnects with pitches from 1-40 μm [6, 7] provide high-bandwidth, minimal latency connections and can reduce total wirelength. With assembly yields consistently demonstrated to be >99% [8], partitioning of large designs into multiple small dies will improve yield, and employment of Known Good Die (KGD) testing before bonding can reduce the total manufacturing cost [9]. Further, heterogeneous process technologies, like DRAM or emerging Non-Volatile Memories, can be tightly integrated with the CMOS logic to greatly improve system performance and efficiency. 3D ICs have come to market over the last several years in a number of products, including CMOS image sensors, stacked High Bandwidth Memory for GPUs, and multi-die high-capacity FPGAs. Although most CMOS logic is still 2D, foundries anticipate that mainstream systems will begin employing 3D integration within the next several years due to demand for footprint, capacity, and efficiency improvement [10]. Further down the road, monolithic 3D integration may provide even higher integration between layers to further improve efficiency and performance [11]. The trend in 3D packaging technologies is shown in Fig. 1.

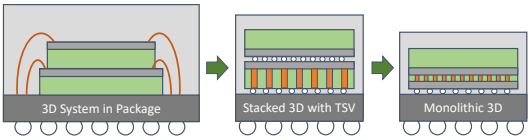

Figure 1: 3D packaging technology is expected to transition from current wire bond SiP to high-bandwidth TSV-based die stacking, and eventually to full monolithic integration.

1.2 General Challenges in 3D IC Design, Fabrication, and Deployment

Although 3D integration offers a range of promising benefits, like all new technologies, it also brings new challenges. Since 3D integration increases the number of transistors per area, it leads to an increase in power density that translates to more difficult thermal management and power delivery. High-performance systems may not be cost-effective in 3D when extra thermal management is considered [12]. However, design automation methods have been developed for thermal-aware 3D floorplanning and 3D power delivery to mitigate these problems [13]. From a process perspective, extra fabrication steps are needed to add TSVs and to perform thinning and bonding, thus incurring additional cost and complex-

GLSVLSI '17, May 10 - 12, 2017, Banff, AB, Canada

ISBN 978-1-4503-4972-7/17/05...5.00

DOI: http://dx.doi.org/10.1145/3060403.3060500

ity. If cost-efficient scaling is desired, these overheads must be less than any yield improvements from fabricating smaller dies. Adding TSVs and multiple layers also requires adjustments to placement and routing tools, and partitioning across dies complicates testing methodology [14]. Finally, the extra complexity of multiple dies and new process steps have so far resulted in a lack of standardization and more complicated supply chains. However, the benefits of 3D integration have attracted significant industry demand and development, and most of these challenges will be resolved as tools and processes mature.

1.3 Contribution of this Work

Previous surveys on utilizing 3D integration for security purposes have addressed the advantages of die-stacking structures in secure split manufacturing [15], enhancing the protection against reverse-engineering [16], and side-channel attacks [17]. However, a majority of the existing work has focused on circuit and architecture level opportunities enabled by 3D IC but has not fully considered the potential security vulnerabilities and technology challenges in secure 3D IC designs.

In this paper, we first summarize the novel opportunities offered by 3D integration for security mechanism in Section 2. Then we list potential security vulnerabilities in 3D ICs in Section 3. To further analyze these security challenges, we formulate new attack models based on our observations in Section 4. We envision that TSVs introduce the vulnerabilities that can be utilized by adversaries to insert hardware Trojans. We also analyze a manufacturing scenario neglected by previous works, in which the full design details of the 3D chip are exposed to the untrusted foundries. Since limited 3D testing techniques are available to detect malicious circuits, we predict that a new form of threat, cross-tier hardware Trojans, is likely to occur. In Section 5, we summarize the state-of-the-art countermeasures against existing security threats in 3D designs and further propose new countermeasures. This work is concluded in Section 6.

2. UNIQUE OPPORTUNITIES THAT 3D STRUCTURE OFFERS FOR SECURITY MECHANISMS

Several existing works have comprehensive summaries on the advantages of 3D IC for security enhancement [15–17]. We classify these unique opportunities according to their applications in different stages of the semiconductor supply chain [18].

2.1 Synthesis and Verification Stage

In this stage, designers can utilize the unique die-stacking architecture of 3D ICs to implement new security features, enhance existing security metrics, or reduce the overhead of security applications.

- In order to incorporate new security features, designers are provided with a wide spectrum of CMOS and non-CMOS technologies thanks to the heterogeneous integration capabilities enabled by die-stacking architecture. For example, CMOS technologies in different process nodes can be integrated, and Physical Unclonable Function (PUF) implemented with non-CMOS technologies can be integrated with CMOS processors.
- To enhance existing security metrics, designers could optionally add a trusted control plane on top of the untrusted compute plane to monitor its behaviors. Since the die-stacking structure allows high-bandwidth communications between these planes, trusted computation can be guaranteed with negligible overhead.
- To reduce the overhead of security applications, die-stacking structures could enable high performance Process-In-Memory encryption to reduce the memory security overhead.

2.2 Fabrication Stage

In this stage, designers can employ the modularity features of the 3D IC for split manufacturing. Split manufacturing is proposed to hinder malicious foundry's efforts to overbuild the IC or insert hardware Trojans. In order to take advantage of the advanced manufacturing capability of the untrusted foundries, the original design is split, and performance-critical parts are fabricated by untrusted foundries and security-critical parts are fabricated by trusted foundries. 3D IC split manufacturing is more suitable compared with conventional 2D Back-End-of-Line (BEOL) and Front-End-of-Line (FEOL) based split manufacturing [19], since 2D design imposes stricter fabrication compatibility among foundries and provides limited design flexibilities. Designers can also utilize Intellectual property (IP)-reuse strategies for cost reduction during split manufacturing, since the secure die containing active components provided by trusted foundries could be reused across a wide range of designs.

2.3 Production Stage

After product shipping, designers can use the 3D IC stacking structures to protect against side-channel leakage and reverse-engineering attacks.

- To defend against side-channel attacks, novel components could be designed to reduce side channel leakage vulnerabilities [17]. For example, the cache could be designed to reduce timing side channel risks and noise generators could be added to reduce thermal side channel leakage.
- To protect against reverse engineering, circuit obfuscation techniques could be utilized to implement 3D IC [16]. For example, a Network-on-Chip (NoC) based shielding plane can be inserted between two commercial dies to thwart reverse engineering attacks on the vertical dimension. Also, Monolithic three-dimensional (M3D) integration can ensure that the layouts of different logic gates show indistinguishable patterns inside a standard cell [17].

3. UNIQUE SECURITY CHALLENGES IN 3D ICS

Although vertical integration brings new opportunities for defenders to address some of the security issues in 2D ICs, it also leaves more space for attackers to compromise 3D chips from various stages in the 3D IC supply chain. A previous work [16] summarizes the hardware security threats in 3D integrated circuits: (1) vertical communication trustworthiness, (2) hardware Trojan mechanisms, and (3) emerging side channel attacks as new security threats with immediate impact in 3D ICs.

Furthermore, existing testing techniques for 3D ICs have own limitations on malicious circuit detection such as: (1) the probe size and the probe pitch distance for mid-bond testing are not small enough for advanced 3D dies [20], (2) test probes may damage the TSVs after testing, causing reliability degradation, and (3) individual die performance and the integrity of vertical interconnects may reduce after final bonding. Due to these testing challenges, malicious components detection through 3D functional testing is not optimistic [15]. Moreover, large process, voltage, and temperature variations within 3D ICs may lead to a high false positive rate for traditional methods that rely on side-channel analysis based hardware Trojan detection.

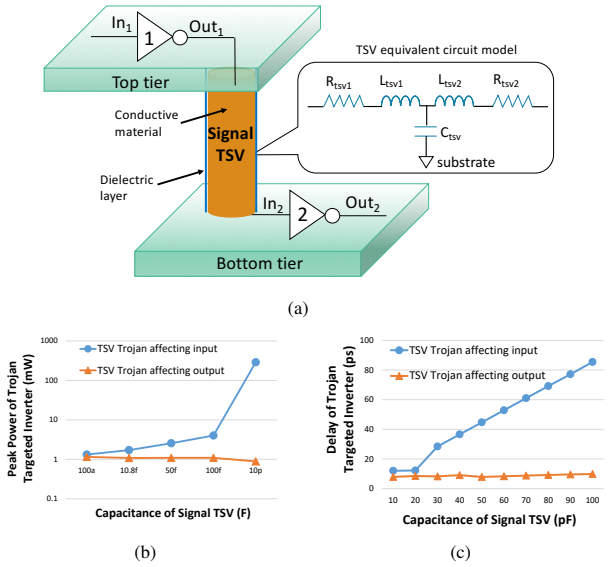

Figure 2: Signal-TSV based parametric hardware Trojan (a) simulation setup, (b) impact of Trojan on peak power, and (c) impact of Trojan on gate delay. Experiments conducted here are based on a 45nm NCSU FreePDK.

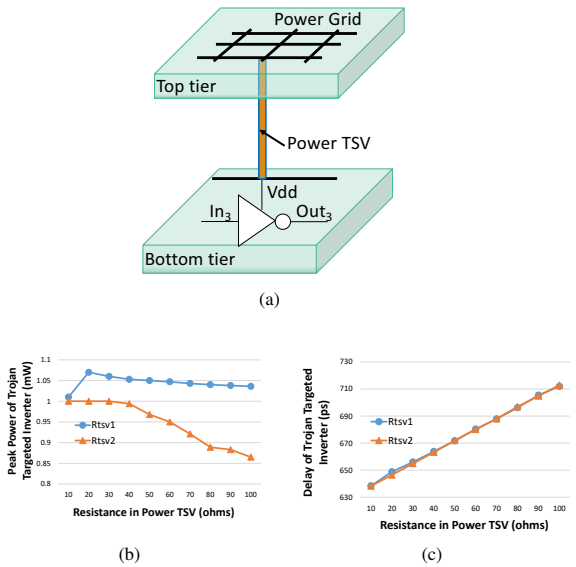

Figure 3: Power-TSV based parametric hardware Trojan (a) simulation setup, (b) impact of Trojan on peak power, and (c) impact on gate delay. Note, R_{tsv1} and R_{tsv2} are the equivalent resistance in the TSV model.

3D integration provides significant advantages in split manufacturing compared with 2D design in terms of fabrication compatibility and flexibility as discussed in Section 2. However, previous research mainly explored how to utilize 3D passive interposers [21] to hide wires and 2.5D passive interposers to hide connection cuts [22]. The circuit is split into trusted tiers which contain lifted metal wires [21] or connections between two outsourced dies [22], and untrusted tiers which contain transistors and the rest of the metal connections. Since only metal wires or connection cuts can be hidden in the passive interposer, to achieve certain degree of security enhancement, considerable amount of metal wires are needed to route through trusted tiers, creating large cut size (thus large micro-bump area). The security of the passive interposer is a serious concern, since reverse engineering can easily reveal the connections of the wires (these wires manufactured by less advanced foundries could easily be figured out). Even worse, the passive interposer can only be fitted to one design, making the cost of the passive interposer expensive and split manufacturing process hard.

4. ATTACK MODELS FOR 3D ICS

In this section, we analyze the security vulnerabilities of 3D ICs induced by the untrusted foundries. We specially target the hardware Trojan insertions scenarios which are unique to 3D chips.

4.1 Attacks from Untrusted Vertical Interconnect Foundry

A stacked 3D IC integrates all the dies with vertical interconnects (e.g. TSVs). In 3D SoCs with diverse dies, each die can be designed and fabricated by trusted vendors. A 3D foundry with TSV manufacturing capability processes and bonds these dies using TSVs. The untrusted manufacturer for vertical interconnect fabrication could introduce hardware Trojans to the TSVs, thus sabotaging the integrity and reliability of the 3D ICs. Due to limited testing coverage achieved by the post-bond testing in 3D ICs, TSV-based Trojans may not be detected during the functional verification. We conducted the basic experiment on signal TSVs and power TSVs to demonstrate the consequence of hardware tampering attacks. We envision that TSVs might be exploited as a parametric hardware Trojan. This means, the untrusted foundry can modify the fabrication process parameters for the TSV fabrication to change the TSV height and dielectric thickness. To model a TSV-based Trojan, we adopt the TSV model as in [23], in which a TSV is equivalent to a RLC network as shown in Fig. 2(a).

Signal-TSV based Hardware Trojan

In TSV-based 3D integration, via-last TSVs are fabricated after the Back-End-of-Line (BEOL). This type of TSV passes through the silicon substrate and the metalization layers, leaving a large exploitation space for hardware Trojan insertion. The triggered Trojan can alter the signal that the Trojan is targeted at. The impact of a Trojan inserted in a signal TSV on the peak power and gate delay is noticeable and varies with the Trojan location, as shown in Fig. 2(b). We swept C_{tsv} and measured the peak power of Inverter 1 and Inverter 2. If the malicious TSV is inserted before the input node of the target (Inverter 2), the peak power of Inverter 2 can increase by more than two orders of magnitudes with the increase of C_{tsv}. However, if the malicious signal TSV is considered as a load for the target (Inverter 1), the peak power of Inverter 1 slightly changes during the course of sweeping C_{tsv}.Therefore, a *signal-TSV based Trojan has more impact as a driver circuit than as a load circuit*. The impact of malicious signal TSVs on the delay of the targeted gate has a similar trend with the peak power, as shown in Fig. 2(c).

Power-TSV based Hardware Trojan

Via-first TSVs are fabricated during the Front-End-of-Line (FEOL). This type of TSV connects the bottom metal layer of the top tier, taking Fig. 3(a) as an example, with the top metal layer of the bottom tier. Via-first TSV is useful for power grid connection. If a power TSV is compromised by a hardware Trojan, the equivalent resistance of the TSV plays a significant role on the peak power and gate delay of the targeted logic gate. We assume that a malicious power TSV provides a Vdd for the inverter in the bottom tier as shown in Fig. 3(a). As we sweep the equivalent resistance of the

TSV, the inverter peak power is reduced by 15% and inverter delay is increased by 11%, as shown in Figs. 3(b) and (c). The changes on power are not negligible for those who take power measurements as side-channel signals.

4.2 Attacks from Untrusted Split Manufacturing Foundry

The split manufacturing foundry fabricates only untrusted tiers. The trusted tiers and the final assembly is carried out in the trusted foundries. Two different assumptions about the adversaries have been proposed by previous work [21, 22]. The first work [21] assumes that a malicious observer exists in the design stage to provide information to a malicious attacker in the foundry. The malicious observer has full knowledge of the circuit but cannot effect any changes. The malicious attacker in the foundry can modify the circuit layout before the chip is fabricated. The second work [22] assumes a weaker attacker who only knows the partial design layout and knows nothing about the complete design. The goal of the attacker is to acquire the whole design to overbuild ICs for profits or insert hardware Trojans to compromise the security of the system at certain time. If only wires are hidden from the untrusted foundries, as assumed by 2D BEOL/FEOL designs and 3D passive interposer-based designs, the attackers can utilize some placement and routing heuristics to guess the hidden connections, such as proximity attacks [22]. If the attacker can acquire the product after shipping, the passive interposer containing only metal wires are vulnerable to physical reverse engineering as well as logic profiling attack since only wires can be hidden.

4.3 Attacks from Untrusted Unified Foundry

The unified foundry fabricates both dies for multiple tiers and the vertical interconnect between tiers. Since the untrusted unified foundry has the full design details of the 3D chip, security benefits from split manufacturing are not achievable in this scenario neither. Reverse engineering, hardware IP piracy, and hardware tampering attacks will be more prevalent in this case. For TSV-based 3D ICs, the die and interconnect manufacturing steps are executed consecutively in the same foundry. To bypass the pre-bond, mid-bond, and post-bond testing, the untrusted unified foundry can collaboratively tamper the existing die design and TSVs in a way that the malicious component will not be active either in the die testing or TSV testing. Due to the limitation of 3D testing techniques, it will be more difficult to detect the untrusted unified foundry's malicious circuit in a 3D IC than in a 2D IC. We predict a new kind of hardware Trojan in this scenario: the cross-tier hardware Trojan, which is a more general Trojan in 3D ICs than the TSV-based hardware Trojan.

In the proposed cross-tier Trojan: (1) *Trojan trigger and payload circuits are not in the same tier*. The cross-tier hardware Trojan #1 in Fig. 4 depicts the conceptual idea. If the trigger circuit is located in another tier, side-channel analysis based Trojan detection methods cannot detect the presence of hardware Trojan during the pre-bond testing on each single die. As a 3D chip integrates a much larger number of transistors, the overhead induced by the Trojan circuit is relatively smaller in 3D ICs than that in 2D ICs. Thus, the separated Trojan trigger and payload circuits will increase the difficulty of Trojan detection. (2) *The Trojan is triggered by multiple trigger circuits, which are distributed in multiple tiers.* As shown in the cross-tier hardware Trojan #2 in Fig. 4, the signals from the top tier, bottom tier, and the vertical interconnect between the top and middle tiers collaboratively drive the trigger circuit for the hardware Trojan in the middle tier. Compared to hardware Trojans in 2D ICs, this type of cross-tier hardware Trojan may have significantly lower Trojan triggering probability.

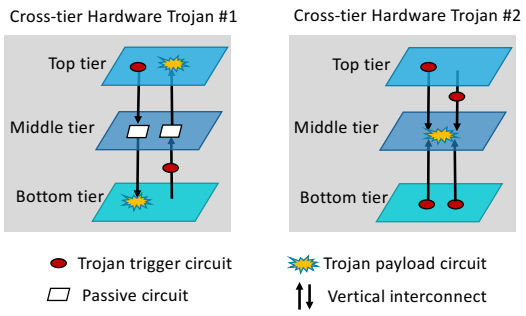

Figure 4: Examples of cross-tier hardware Trojans in TSV-based 3D ICs.

5. STATE-OF-THE-ART METHOD REVIEW

In this section, we review the existing countermeasures against the different threats in 3D integration. Further, we propose possible hardware Trojan detection and mitigation methods.

5.1 Split Manufacturing

The threats considered in this countermeasure are Reverse Engineering at untrusted foundry. As indicated by leading 3D manufacturing foundries [24], 3D ICs facilitate *split manufacturing* where the entire IC is distributed throughout multiple dies/planes. Due to the incompleteness of each layer, it is difficult for the attackers to reverse engineer the entire design from one die.

Existing 3D split manufacturing approaches fall into two primary categories. In the first category, as investigated in [25–27], the entire design is separated into two tiers: one plane is dedicated as the primary computation plane whereas the second plane is an optional control plane that should be provided by a trusted foundry. This control plane is used to monitor possible malicious behavior within the computation plane and overwrites the malicious signals, if necessary.

The second category, as studied by Imeson *et al.* [21], relies on interconnects of a trusted tier to obfuscate the entire 3D circuit. Thus, the circuit within the untrusted tier cannot be reverse engineered since interconnectivity is unknown. Similar studies have been performed that investigate methods to further enhance the obfuscation level achieved by split manufacturing [22, 28–30]. Some examples include layout-level techniques [28], heuristic attack [29], cell placement [30], circuit size cut algorithm and secure interposer layout [22]. These existing works prevent reverse engineering from retrieving the original circuit.

5.2 Camouflaging in Monolithic 3D ICs

The security threats target in this countermeasures are IP piracy and reverse engineering. The concept of camouflaging gates in monolithic three-dimensional (M3D) is presented in [17]. The main goal of this approach is to make M3D IC secure with smaller overhead. The camouflage IC can be classified into two categories. The first category addresses intra-standard cell camouflage where standard cells are redesigned to look identical by inserting dummy vias. The identical gates provide different functionalities. The other category addresses inter-standard cell camouflage where dummy circuits are filled in the empty spaces among standard cells [10, 12] such that the attackers cannot figure out standard cell parts. Authors suggested improvements in M3D IC context to minimize

the overhead. The overhead of intra-camouflaged standard cells, is mainly due to extra wiring inside of the standard cell. This drawback could be alleviated using fine-grained inter-layer vias. For inter-standard cell camouflage, the authors proposed four different partition options for filling up the dummy cells to escalate the reverse engineering efforts of attackers.

5.3 Transistor Locking in Monolithic 3D ICs

Alternatively, IP piracy and reverse engineering attacks can be addressed by logic locking techniques. The work in [31] investigates a novel transistor-level logic locking method to address the security challenges in monolithic three-dimensional (M3D) ICs. This method locks logic gates by independently inserting parallel or serial locking transistors and camouflaged contacts in multiple tiers. The locking keys are only available to authorized users. The application of a wrong key to the locked functional block either leads to a logic malfunctions by opening or shorting pull-up or pull-down network or it significantly changes the power profile. Furthermore, the contact camouflaging is exploited to thwart image-analysis based reverse engineering attacks.

5.4 Techniques against Thermal Signal based Side-Channel Attacks

Thermal Side-channel (TSC) attacks [17] have been shown to disclose the activities of key functional blocks and even encryption keys by built-in thermal sensors, external attached thermal sensors, or high resolution thermal imaging. A previous work [32] proposes to protect ICs from thermal side-channel attacks by utilizing intrinsic characteristics of 3D chip integration, as well as proactively using dynamic shielding patterns to conceal critical activities on chip. The design includes a micro-controller unit that dynamically generates complementary activity patterns to prevent side-channel data leakage. Thermal patterns are generated in a randomized, non-repeating manner such that side-channel attackers cannot extract meaningful information by observing any pattern sequence. The proposed architecture covers all thermal sensor placement options such that noise injected by security layers will decrement the side-channel leakage of any critical areas.

5.5 Network-on-Chip based Shielding Plane (NoCSIP)

A novel network-on-chip based 3D obfuscation method is proposed in [16] to thwart reverse engineering attacks in TSV-based 3D ICs. The authors proposed to use a Network-on-Chip based shielding plane (NoCSIP) for cross-plane communication (i.e. vertical communication channel). The essence of NoCSIP is to provide an obfuscated communication channel between two planes that host commercial dies and block the direct communication between two commercial dies in a 3D structure. This NocSIP method makes it significantly more challenging to reverse engineer the 3D system. If the proposed shielding layer is sufficiently strong, the 3D system has more flexibility to use low end dies without sacrificing the overall system's security assurance.

5.6 Possible 3D Trojan Detection and Mitigation Methods

One low-cost countermeasure against the potential hardware Trojans inserted by the untrusted vertical interconnect foundry discussed in 4.1 is shown in Fig. 5(a). Each single die needs extra work to swap connections between the top metal layer and the TSVs. For instance, the single die is fabricated in trusted foundry and the 3D integration foundry intends to implement a parametric hardware Trojan for instance, on a clock TSV. A clock-TSV is the inter-die

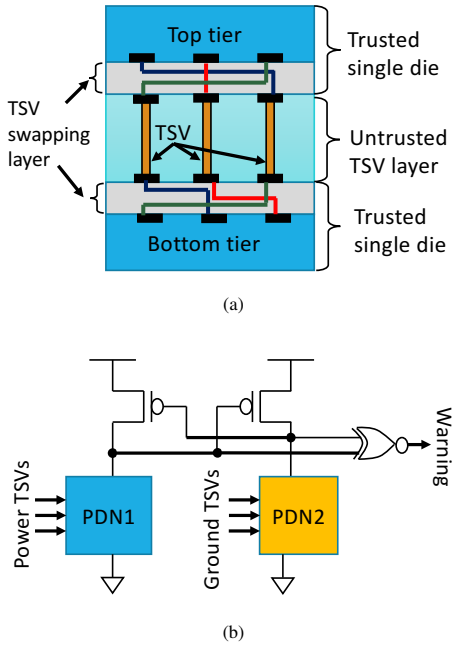

Figure 5: Possible countermeasures for 3D hardware Trojans. (a) TSV swapping, and (b) DCVSL-based abnormal power and ground grid detection.

connection between the clock networks on vertically adjacent tiers. By swapping the metal-to-TSV connection, the designed parametric Trojan could be placed to a signal TSV instead. Thanks to logic masking and inherent noise filtering of digital circuits, that parametric Trojan is very likely to be muted. The parametric hardware Trojans on the TSV will not cause a catastrophic effect on the clock network.

Differential Cascade Voltage Switch Logic (DCVSL) gates takes complementary inputs and generate complementary outputs. We can exploit the complementary characteristic to detect the abnormal power and ground voltages induced by malicious power and ground TSVs, as shown in Fig. 5(b). Once the multiple power/ground lines do not reach to the standard voltage, the outputs of the DCVSL gate are not complementary and thus the warning signal goes to high. This warning signal can be further used to alert the 3D chip user.

If 3D NoC is adopted in the 3D chip, we can also exploit obfuscated routing algorithms for the 3D switches to eliminate the explicit vertical communication between tiers.

6. CONCLUSION

Due to limited testing techniques, 3D ICs are expected to have new security threats than those existed in 2D ICs. Previous studies on 3D IC security mainly focus on the methods that leverage 3D structures to address the security concerns on 2D ICs, rather than understanding the security vulnerabilities inherently existed in 3D ICs. In this work, we first summarized the novel opportunities offered by 3D integration for security mechanism and then enlist the potential security vulnerabilities in 3D ICs. TSV-based 3D hardware Trojans and cross-tier hardware Trojans , which are unique to 3D chips, are discussed. Further, we reviewed several countermeasures against existing security threats and propose potential 3D Trojan detection and mitigation methods.

The countermeasures for new security threats on 3D ICs should be investigated by hardware security community. In future work,

we will implement the possible countermeasures and assess the countermeasure's resistance against hardware Trojan and reverse engineering attacks from untrusted foundries.

7. REFERENCES

[1] L. Labrak and I. O'Connor, "Heterogeneous System Design Platform and Perspectives for 3D Integration," *Proc. of the IEEE International Conference on Microelectronics*, pp. 161–164, December 2009.

[2] L. Xue, *et al.*, "Three-Dimensional Integration: Technology, Use, and Issues for Mixed-Signal Applications," *IEEE Transactions on Electron Devices*, Vol. 50, No. 3, pp. 601–609, March 2003.

[3] Y. Xie and J. Zhao, *Die-stacking Architecture*. Morgan & Claypool Publishers, 2015.

[4] Y. Xie, J. Cong, and S. Sapatnekar, *Three-Dimensional Integrated Circuit Design: EDA, Design and Microarchitectures*, 1st ed. Springer Publishing Company, Incorporated, 2009.

[5] J. Zhao, Q. Zou, and Y. Xie, "Overview of 3D Architecture Design Opportunities and Techniques," *IEEE Design Test*, Vol. PP, No. 99, pp. 1-1, 2015.

[6] K. W. Lee, *et al.*, "Novel reconfigured wafer-to-wafer (W2W) hybrid bonding technology using ultra-high density nano-Cu filaments for exascale 2.5D/3D integration," *2015 IEEE International Electron Devices Meeting (IEDM)*, pp. 8.2.1-8.2.4, Dec 2015.

[7] P. Vivet, *et al.*, "3D advanced integration technology for heterogeneous systems," *2015 International 3D Systems Integration Conference (3DIC)*, pp. FS6.1-FS6.3, Aug 2015.

[8] C. C. Lee, *et al.*, "An Overview of the Development of a GPU with Integrated HBM on Silicon Interposer," *2016 IEEE 66th Electronic Components and Technology Conference (ECTC)*, pp. 1439-1444, May 2016.

[9] D. Stow, *et al.*, "Cost analysis and cost-driven IP reuse methodology for SoC design based on 2.5D/3D integration," *2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pp. 1-6, Nov 2016.

[10] S. Hou, "Interposer Technology: Past, Now, and Future," 2016, semicon Taiwan.

[11] J. Shi, *et al.*, "A 14nm FinFET transistor-level 3D partitioning design to enable high-performance and low-cost monolithic 3D IC," *2016 IEEE International Electron Devices Meeting (IEDM)*, Dec 2016.

[12] D. Stow, *et al.*, "Cost and Thermal Analysis of High-Performance 2.5D and 3D Integrated Circuit Design Space," *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pp. 637-642, July 2016.

[13] W. L. Hung, *et al.*, "Interconnect and thermal-aware floorplanning for 3D microprocessors," *Proc. of ISQED'06)*, pp. 6 pp.-104, March 2006.

[14] Y. Chen, D. Niu, Y. Xie, and K. Chakrabarty, "Cost-effective integration of three-dimensional (3D) ICs emphasizing testing cost analysis," *2010 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pp. 471-476, Nov 2010.

[15] Y. Xie, *et al.*, "Security and Vulnerability Implications of 3D ICs," *IEEE Transactions on Multi-Scale Computing Systems*, Vol. 2, No. 2, pp. 108-122, April 2016.

[16] J. Dofe, Q. Yu, H. Wang, and E. Salman, "Hardware Security Threats and Potential Countermeasures in Emerging 3D ICs," *Proc. of GLSVLSI '16*, pp. 69–74, 2016.

[17] P. Gu, *et al.*, "Leveraging 3D Technologies for Hardware Security: Opportunities and Challenges," *Proc. GLSVLSI '16*, pp. 347–352, 2016.

[18] M. Rostami, F. Koushanfar, and R. Karri, "A primer on hardware security: Models, methods, and metrics," *Proceedings of the IEEE*, Vol. 102, No. 8, pp. 1283–1295, 2014.

[19] Y. Xie, C. Bao, and A. Srivastava, "3D/2.5 D IC-Based Obfuscation," *Hardware Protection through Obfuscation*. Springer, 2017, pp. 291–314.

[20] E. J. Marinissen, "Challenges and emerging solutions in testing TSV-based 2 1 over 2D- and 3D-stacked ICs," *Proc. of DATE '12*, pp. 1277-1282, March 2012.

[21] F. Imeson, A. Emtenan, S. Garg, and M. V. Tripunitara, "Securing Computer Hardware Using 3D Integrated Circuit (IC) Technology and Split Manufacturing for Obfuscation." *USENIX Security*, Vol. 13, 2013.

[22] Y. Xie, C. Bao, and A. Srivastava, "Security-Aware Design Flow for 2.5 D IC Technology," *Proc.of TrustED '15*, pp. 31–38, 2015.

[23] R. S. Jagtap, "A Methodology for Early Exploration of TSV Interconnects in 3D Stacked ICs," Master's thesis, Delft University of Technology, Netherlands, 2011.

[24] S. Bansal, "3D IC Design," *EETimes (Nov 14, 2011), http://www.eetimes.com/document.asp?doc_id=1279081*, 2011.

[25] M. Bilzor, "3D execution monitor (3D-EM): Using 3D circuits to detect hardware malicious inclusions in general purpose processors," *Proc. of the 6th International Conference on Information Warfare and Security*, p. 288. Academic Conferences Limited, 2011.

[26] J. Valamehr, *et al.*, "A 3-D Split Manufacturing Approach to Trustworthy System Development," *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, Vol. 32, No. 4, pp. 611–615, 2013.

[27] T. Huffmire, *et al.*, "Hardware trust implications of 3-D integration," *Proc. of the 5th Workshop on Embedded Systems Security*, p. 1. ACM, 2010.

[28] K. Xiao, D. Forte, and M. M. Tehranipoor, "Efficient and secure split manufacturing via obfuscated built-in self-authentication," *Hardware Oriented Security and Trust (HOST), 2015 IEEE International Symposium on*, pp. 14–19. IEEE, 2015.

[29] J. Rajendran, O. Sinanoglu, and R. Karri, "Is split manufacturing secure?" *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2013*, pp. 1259–1264. IEEE, 2013.

[30] M. Jagasivamani, *et al.*, "Split-fabrication obfuscation: Metrics and techniques," *Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium on*, pp. 7–12. IEEE, 2014.

[31] J. Dofe, *et al.*, "Transistor-level camouflaged logic locking method for monolithic 3D IC security," *2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)*, pp. 1-6, Dec 2016.

[32] P. Gu, *et al.*, "Thermal-aware 3D design for side-channel information leakage," *2016 IEEE 34th International Conference on Computer Design (ICCD)*, pp. 520-527, Oct 2016.