Hardware Security Threats and Potential Countermeasures in Emerging 3D ICs

Jaya Dofe
Qiaoyan Yu
Department of Electrical and Computer Engineering
University of New Hampshire
Durham, NH 03824
<jhs49, qiaoyan.yu>
@unh.edu

Hailang Wang
Emre Salman
Department of Electrical and Computer Engineering
Stony Brook University
Stony Brook, NY 11794
<hailang.wang, emre.salman>
@stonybrook.edu

ABSTRACT

New hardware security threats are identified in emerging three-dimensional (3D) integrated circuits (ICs) and potential countermeasures are introduced. Trigger and payload mechanisms for future 3D hardware Trojans are predicted. Furthermore, a novel, network-on-chip based 3D obfuscation method is proposed to block the direct communication between two commercial dies in a 3D structure, thus thwarting reverse engineering attacks on the vertical dimension. Simulation results demonstrate that the proposed method effectively obfuscates the cross-plane communication by increasing the reverse engineering time by approximately 5× as compared to using direct through silicon via (TSV) connections. The proposed method consumes approximately one fifth the area and power of a typical network-on-chip designed in a 65 nm technology, exhibiting limited overhead.

Categories and Subject Descriptors

B.7 [**Integrated Circuits**]: VLSI (very large scale integration)

Keywords

3D ICs, hardware security, Network-on-Chip

1. INTRODUCTION

Three-dimensional (3D) integration has attracted significant attention during the past two decades to develop diverse computing platforms such as high performance processors, low power systems-on-chip (SoCs), and reconfigurable platforms such as FPGAs. Despite the well-understood advantages over 2D integrated circuits (ICs), 3D ICs introduce unique and unexplored challenges on managing hardware security. Unfortunately, existing work on hardware security of 3D ICs primarily focuses on methods to leverage 3D characteristics to resolve the security challenges of 2D ICs, rather than studying the security threats and corresponding countermeasures in 3D ICs.

One of the significant challenges is ensuring *inter-die security* within a heterogeneous 3D stack. For example, a 3D IC consisting of multiple dies from different vendors (as in the plug-and-play based 3D integration) suffers from trustworthiness since different intellectual property (IP) providers may not follow the same regulations and conduct the same degree of die authentication. Integrating dies from third-party vendors by utilizing an interposer based 2.5D technology is already a common practice. This trend is expected to grow, particularly for 3D SoCs where multiple functionalities coexist. Thus, inter-die security is expected to be a serious concern for emerging 3D ICs. These challenges are identified in this paper and potential solutions are proposed to enhance hardware security within 3D ICs.

The rest of the paper is organized as follows. Existing hardware security threats and typical countermeasures are summarized in Section 2. Three important security threats are introduced for 3D ICs in Section 3. A potential countermeasure is proposed in Section 4 to address reverse engineering attacks on vertical communication channels. Simulation results are provided in Section 5. The paper is concluded in Section 6.

2. BACKGROUND

2.1 Security Threats and Countermeasures in 2D ICs

Hardware security threats on traditional 2D ICs are primarily from hardware Trojan horse [1], side-channel analysis attacks [2], fault attacks [3], counterfeit chips [4], and reverse engineering induced loss of IP piracy [5]. Hardware Trojan models and general detection methods have been well studied in existing literature [1, 6, 7].

Side-channel analysis (SCA) attacks [2] aim to retrieve the secret key in cryptosystems by analyzing the power and delay characteristics of the IC. The most common countermeasures for SCA attacks are random masking techniques [8], insertion of dummy code, power consumption randomization, and balancing the data.

Fault attacks can compromise the cipher implementation and produce faulty ciphertexts for cryptanalysts to retrieve the secret key [3, 9]. White light, laser beams, voltage glitches, and temperature control are possible manipulation means to perform fault attacks [10]. Existing countermeasures for fault attacks are primarily based on error detection or/and correction codes [11, 12].

GLSVLSI '16, May 18-20, 2016, Boston, MA, USA

DOI: http://dx.doi.org/10.1145/2902961.2903014

Methods to identify counterfeit chips and IP piracy have also been well studied [4, 5]. Vertical integration brings a new dimension to the counterfeit design. In addition to the protection of each die, the trustworthiness of the vertical connections/communication should also be ensured.

2.2 Existing Work on Hardware Security for 3D ICs

Majority of the existing work leverages the unique 3D characteristics to enhance security of 2D ICs rather than investigating hardware security within stand-alone 3D ICs. As indicated by leading 3D manufacturing foundries [13], the stacking process of 3D ICs conceals the details of the circuit design and therefore thwarts reverse engineering. Secondly, 3D ICs facilitate *split manufacturing* where the entire IC is distributed throughout multiple dies/planes. Thus, due to the incompleteness of each plane, design details of a functional block are not revealed.

Existing 3D split manufacturing approaches fall into two primary categories. In the first category, as investigated by Valamehr *et al.* [14], 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.* [15], relies on interconnects of a trusted die 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 to further enhance the obfuscation level achieved by split manufacturing [16–18].

As exemplified by these studies, existing approaches rely primarily on the presence of a trusted plane. While effective to enhance security, these existing techniques do not investigate the potential security weaknesses inherent to 3D ICs.

3. NEW SECURITY THREATS IN 3D ICS

One of the primary limitations of existing work is that the trustworthiness of the vertical communication process is taken for granted. This assumption leaves a critical component of 3D integration insecure. In this section, new security threats induced by 3D integration are introduced.

3.1 Trustworthiness of Vertical Communication

A nontrivial security weakness within 3D ICs is the trustworthiness of vertical communication. In a heterogeneous 3D stack with dies from different vendors, one of the dies can attempt to extract secret information such as an encryption key, authentication code, or certain IP characteristics. Thus, a die within a 3D stack should not only be protected from external attacks (as is the case in traditional 2D ICs), but also from attacks originating from a nearby die within the same 3D stack. Furthermore, since the authentication level of each die is different, the security of the overall 3D IC is dependent upon the weakest die. The overall 3D IC (including the die with a strong authentication level) can be compromised once an attacker succeeds in accessing the weak die. Note that due to high bandwidth inter-die vertical communication, an attacker has more access points to compromise security, producing additional security threats that do not exist in 2D ICs.

Another potential weakness is the leak of connectivity information from an untrusted 3D integration foundry. Existing approaches that rely on split manufacturing typically assume that the vertical communication is inherently secure. Unfortunately, this assumption is not always accurate. For example, the foundry that manufactures vertical interconnects may leak this connectivity information, resulting in weaker design obfuscation than what is assumed with split manufacturing. Existing work has indicated that the straightforward split manufacturing suffers from proximity attack [17].

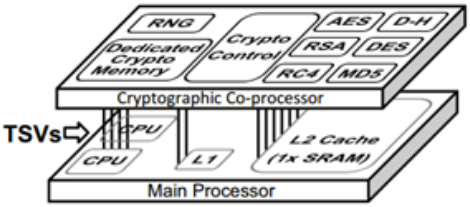


Figure 1: **Secure crypto plane in 3D ICs [21].**

3.2 Potential Trigger and Payload Mechanisms for Hardware Trojans

Due to limited and immature design-for-test techniques for 3D integration, it is more challenging to detect hardware Trojans in 3D ICs. Furthermore, attackers have new design space to hide hardware Trojans. For example, in 2.5D integration, an interposer plane can be exploited to generate a Trojan that is harder to detect. Assume a malicious interconnect within the interposer plane that connects two TSVs together through a switch transistor, fabricated within a die above the interposer. The switch transistor can be activated through a thermal sensor, short circuiting the two distinct TSVs. Thus, a payload mechanism can be as simple as a short wire and a switch transistor.

Another characteristic of 3D ICs that can be exploited by attackers is the poor thermal conductivity. Hardware aging induced metal disconnect and transistor threshold voltage shifting are well-known reliability concerns that accelerate at higher temperatures. Thus, an attacker can insert resistive based heat generation units that accelerate certain reliability mechanisms. This kind of Trojan triggering mechanism is highly challenging to be recognized at the die-level (pre-bond) test or at the final system test stage. Furthermore, due to the immaturity of 3D test mechanisms, hardware Trojan payloads such as voids and partially filled TSVs can generate denial-of-service.

3.3 Side-Channel Analysis Attacks

To retrieve the secret crypto key, side-channel attacks exploit the correlation between the measured side-channel signals (such as delay and power) and the suspected secret key to reduce the number of brute-force attempts. Studies in [19, 20] prove that key retrieval is possible through the analysis of crypto execution times. Side-channel attack can even be done remotely by merely invoking a crypto operation on another machine and measuring the varying execution time [20].

The variation characteristics of 3D ICs add noise to the side-channel signals, thereby blurring the relationship between side-channel signals and the real key. Split manufacturing technique suggests separating the system functions to multiple planes. For instance, as shown in Fig. 1, a separate layer is used for cryptographic operation. These mechanisms, however, cannot completely thwart side-channel attacks. If an attacker can perceive the power measurement of crypto engine by muting other system operations, the well-known power-based SCA methods [22] can be applied to 3D ICs. In another example [23], authors can retrieve the high nibble of key byte in both 2D and 3D cache configurations through delay measurement.

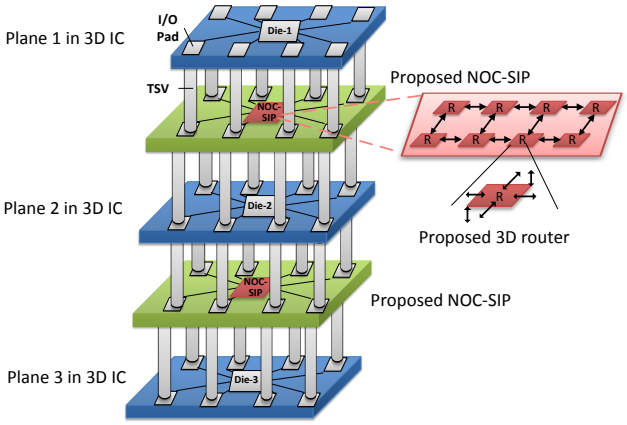


Figure 2: **Conceptual representation of the proposed countermeasure for 3D IC security.**

4. PROPOSED COUNTERMEASURE TO THWART REVERSE ENGINEERING IN 3D ICS: NOC-SIP

The proposed countermeasure is fundamentally different from the split manufacturing approach, where one of the dies and vertical connections must be manufactured by a trusted foundry. Without this assumption, split manufacturing cannot ensure the trustworthiness of a 3D SoC with dies from different vendors. It is predicted that commercial dies, rather than customized dies, will be vertically integrated to develop 3D ICs in the near future. Since the I/O definition and certain specifications of commercial dies are public, an attacker can reverse engineer the 3D SoC design, particularly if each die of the 3D IC can be separated from the stack using a debonding technique. To eliminate the need for at least one trusted foundry for 3D ICs, a secure cross-plane communication network is proposed.

4.1 Overview of the Proposed Method

The proposed method is based on the insertion of a *Network-on-Chip (NoC) based shielding plane* between two commercial dies to thwart reverse engineering attacks on the vertical dimension. As shown in Fig. 2, the proposed NoC shielding plane (NOC-SIP) obfuscates the communication among the adjacent dies.

As compared to the split manufacturing, this method provides higher flexibility and scalability when developing secure 3D ICs. This characteristic is due to the enhanced modularity and scalability of NoCs as compared to a bus centric communication network. Ad-hoc algorithms that split IC functionalities are not suitable for a large-scale system. Furthermore, additional wire lifting through split manufacturing leads to a larger number of TSVs, resulting in more area overhead and TSV capacitance (and therefore power).

The proposed countermeasure aims to address the reverse engineering attack in 3D ICs. We assume that the design in one of the dies could have utilized some obfuscation methods. However, as two dies are integrated in the same package through TSVs, we argue that it is easier to perform sniffing attacks through internal connection in 3D ICs than through external I/O pads. In practice, a 3D chip designer may combine both high-end and low-end dies to reduce the overall cost of a 3D stack. In 2D ICs, the security vulnerability is determined by a single die. Whereas in 3D ICs, the security of the entire system is determined by the weakest die. If the security of the cross-plane communication cannot be assured, the trustworthiness of the heterogeneous 3D stack cannot be guaranteed.

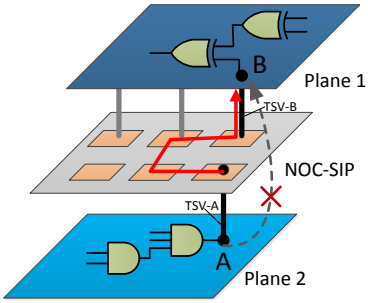


Figure 3: **An example of vertical communication through the proposed NOC-SIP.**

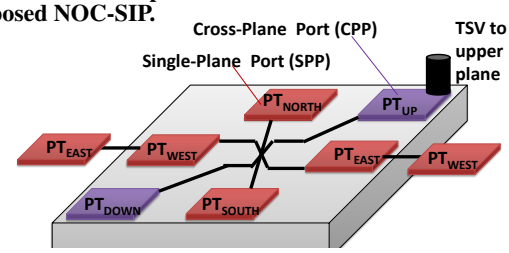


Figure 4: **Proposed 3D router architecture.**

The essence of the proposed NOC-SIP is to provide an obfuscated communication channel between two planes that host commercial dies. Our 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. We assume each commercial die has a regular I/O pad map. Those I/O pads are connected to the proposed NOC-SIP with a regular node array, as shown in Fig. 2. Therefore, the specific I/O connectivity information of the dies is hidden to the 3D foundry. As a result, the proximity attack [17] is less likely to help to reveal the design details from split dies.

An example of the proposed method is depicted in Fig. 3. Without the proposed NOC-SIP die, the node A in plane 2 would be connected to the node B in plane 1 directly through a TSV. If an attacker has the ability to reverse engineer debonded planes 1 and 2, the 3D IC would be compromised. Alternatively, the NOC-SIP plane redirects the signal from a TSV-A on A to several routing hops before the signal truly reaches TSV-B on B. Thus, the direct connection from A to B is removed. The proposed NOC-SIP enhances security for the following three reasons: (1) even if the adversary successfully separates planes 1 and 2, a scanning electron microscope (SEM) picture of the vertical connection does not reveal useful information for reverse engineers to retrieve the complete system design, (2) the inserted NOC-SIP facilitates the use of 2D security countermeasures to address 3D security threats, and (3) the inherent scalability of the NOC-SIP overcomes the limited flexibility and scalability concerns in the existing split manufacturing algorithms.

4.2 Proposed 3D Router Design

4.2.1 *Difference between Typical 2D Router and Proposed 3D Router*

The proposed 3D router is shown in Fig. 4. The single-plane ports (SPP) PT_{North}, PT_{East}, PT_{South}, and PT_{West} fulfill the communication function within the NOC-SIP. Alternatively, the two cross-

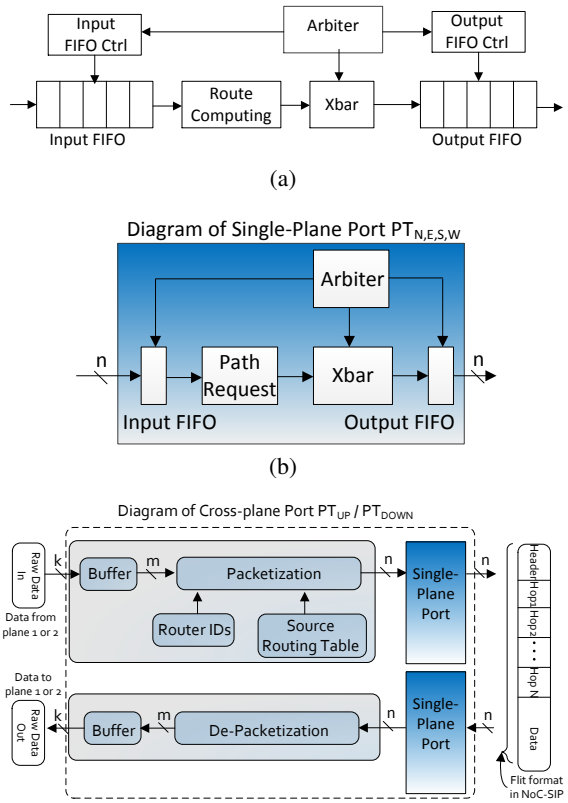


Figure 5: **Schematics of (a) one pair of input and output ports in a 2D router, (b) single-plane port in the proposed 3D router, and (c) cross-plane port in the proposed 3D router.**

plane ports (CPP) PT_{UP} and PT_{DOWN} are responsible for cross-plane communication. In contrast, a typical 2D router has five pairs of input and output ports. Fig. 5(a) shows the diagram of one input and one output port for a 2D router. The proposed 3D router in the NOC-SIP is different than the router in the traditional 2D NoC. As shown in Fig. 5(b), the logic of the input and output ports in our 3D router is much simpler than that of 2D router. Only single-depth input and output FIFO are required; FIFO controllers are removed; route computing unit is replaced with a simple routing path request unit (no computation inside); a simpler arbiter can fulfill the routing arbitration. Among the five ports in a 2D router, one port is connected with a network interface (NI) to reach a processing element (e.g. microprocessor or a memory core). However, in the NOC-SIP, no processing element is connected to any port of the 3D router. The packetization function executed in the NI of a 2D NoC is part of our vertical router's function.

4.2.2 *Router Ports for Vertical Connection*

In our 3D router, the cross-plane ports, PT_{UP} and PT_{DOWN}, are designed for vertical connection from/to other planes. The primary functions of these two ports include: (1) packetize/de-packetize the bit stream from/to the other plane, (2) assign a source-routing path for each data packet, and (3) buffer the bit stream if the previous packets do not have available bandwidth.

As shown in Fig. 5(c), k-bit data from plane 1 is stored in the buffer before packetization. The packet leaving the cross-plane port is formatted in a way that starts with header information, follows with the detailed routing hops, and ends with the real data. The uniqueness of this cross-plane port is the existence of a router identifier (that is programmable after fabrication) and source routing table, which are provided by the 3D chip designer through one-time read-only-memory (ROM) programming equipment. As the router identifier and routing table are initialized after fabrication, placing malicious hardware in the NOC-SIP during the design stage cannot guarantee system compromise. Similarly, the knowledge of the 3D router design does not help the reverse engineer, as the router identifier and source routing table are unknown before deployment. Once the router ID or the source routing table is changed, the secret information sniffed by the attack for one case would not be useful.

4.2.3 *Dynamic Source Routing for Obfuscation*

Source routing introduces unpredictability for the adversary who intends to insert hardware Trojans in the NOC-SIP. As there is no computation unit for route path preparation, the attacker cannot successfully execute a meaningful attack without the knowledge of router identifier assignment. Another advantage of source routing is to manually balance the latency for the transmission between different pairs of I/O pads on planes 1 and 2, shown in Fig. 2. To thwart the delay-based side-channel attacks, the source routing design in the 3D router further facilitates a dynamic routing, which varies the latency of the communication between source and destination ports within the NOC-SIP.

5. SIMULATION RESULTS

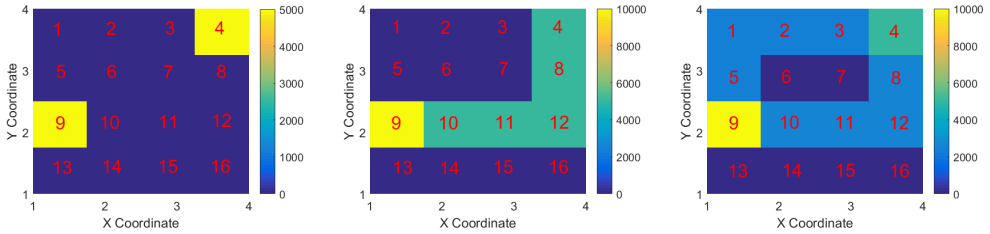
We implemented the proposed NOC-SIP in Verilog HDL and synthesized the HDL code in Synopsys Design Compiler with a 65 nm TSMC technology. The width of the raw data from a plane (other than NOC-SIP) is set to 5 bits, and the packet width for the NOC-SIP is 32 bits. The input and output FIFOs are 32-bit single-depth buffer. XY routing algorithm is applied to the 2D NoC design. Round-robin arbitration is used in both 2D NoC and NOC-SIP. The NI for the 2D mesh NoC is OCP-IP compatible [24]. The hardware cost of our NOC-SIP is compared with two typical 4×4 mesh NoCs.

5.1 Router Activity

The router switching activity of the NOC-SIP is used as a metric to evaluate the difficulty of identifying vertical connectivity through reverse engineering. Three cross-plane communication methods are compared: direct TSV, NOC-SIP with XY routing, and NOC-SIP with source routing. Direct TSV refers to the case where the I/O pads from different dies are statically connected during the 3D IC integration process. NOC-SIP with XY and source routing stand for the proposed shielding layer using XY packet routing and dynamic source routing, respectively.

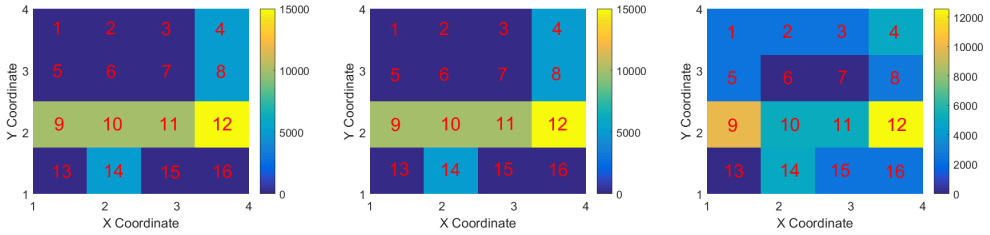
First, we randomly select a single pair of I/O pads from two planes for vertical communication. The number of switching transitions of each 3D router is recorded in 5000 clock cycles. As shown in Fig. 6(a), the activity of the TSVs directly connected to two I/O pads indicates that the TSV nodes 4 and 9 are used in the cross-plane communication. Note that the color bar represents the number of node transitions in 5000 cycles. Alternatively, the router activity map [Fig. 6(b)] of the NOC-SIP with XY routing shows that the routers 4, 8, 9, 10, 11, and 12 are used in the cross-plane communication. A reverse engineer, however, cannot know which two TSVs in the routers are actually used for cross-plane communication. The use of source routing further increases the number of involved routers to 10, thereby increasing the degree of obfuscation, as shown in Fig. 6(c).

If two pairs of vertical communication are applied, the NOC-SIP achieves enhanced obfuscation performance. As shown in Fig. 7, the number of active routers in the NOC-SIP is always greater than the direct TSV method. The source routing for NOC-SIP has



(a) (b) (c)

Figure 6: **Single pad-to-pad vertical communication. (a) Direct TSV, (b) NOC-SIP with XY routing, and (c) NOC-SIP with source routing.**



(a) (b) (c)

Figure 7: **Double pad-to-pad vertical communication. (a) Direct TSV, (b) NOC-SIP with XY routing, and (c) NOC-SIP with source routing.**

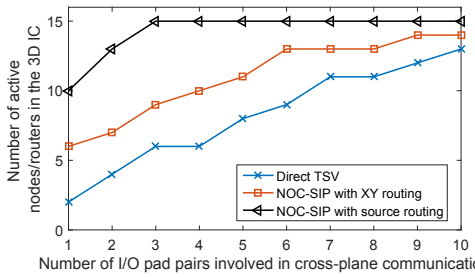


Figure 8: **The number of active routers versus the number of routers having incoming data.**

the ability to distribute the data transmission throughout the entire NOC-SIP. Thus, the proposed approach makes reverse engineering significantly more difficult.

The experiments shown by Figs. 6 and 7 are extended by increasing the number of communication pad pairs to 10. As shown in Fig. 8, the NOC-SIP with source routing engages 12 routers with two pairs of pads. In contrast, the direct TSV method involves 12 routers with 10 pairs of pads. This behavior demonstrates that the proposed NOC-SIP method effectively obfuscates the cross-plane communication by increasing the reverse engineering time by approximately 5× as compared to using direct TSV connections. The direct TSV is the most vulnerable method against reverse engineering on vertical connections.

5.2 Area, Delay and Power Comparison

Since the same topology (mesh) is used in the 2D NoC and NOC-SIP, the area and worst-case delay within a router (i.e. a single node) are compared. The conclusion obtained from this analysis is valid for the entire network. As listed in Table 1, the proposed NOC-SIP with source routing (XY routing) consumes 82% (86%) less area than the 2D NoC in [24]. We added the typical 2D router design and the NI presented in [25] as another reference point. Proposed NOC-SIP with source routing reduces the area overhead by 86% as compared to [25] . The source routing results in more area overhead because of the large source routing table in the cross-plane routers.

Table 1: Area and the Worst-case Delay Comparison, *: Source routing, #: XY routing.

	Single node at 2D NoC		Single node at 3D NoC-SIP	
Modules	Area (μm^2)	Critical Delay (ns)	Area (μm^2)	Critical Delay (ns)
Input FIFO	4122	0.09	288	0.07
Output FIFO	3323	0.33	262	0.07
Route computing	81	0.26	50	0.08
Arbiter	4257	0.69	5298	0.12
NI	19133 [24]	–	–	–
Packetization for cross plane communication	–	–	2962*	0.12*
			719#	0.12#
Total	60517 [24]	0.69	10916*	0.12*
	66508 [25]	0.69	8673#	0.12#

Table 2: Power Consumption Comparison.

On-chip communication network		Power Consumption	
		Dynamic (mW)	Leakage (μW)
Single node at 2D NoC	Router	30.6	187.9
	NI [24]	6.491	
Single node at 3D NOC-SIP with source routing		7.8	46.5
Single node at 3D NOC-SIP with XY routing		7.5	35.3

Since the worst-case delay for the 2D NoC is 0.69 ns, we set the clock frequency to 1.25 GHz for all designs under comparison. The comparison listed in Table 2 indicates that the power consumption of the proposed NOC-SIP with source routing (XY routing) is only 21% (20%) of the 2D NoC.

6. CONCLUSIONS

Existing works have demonstrated that 3D integration provides additional security defense to thwart hardware attacks in 2D ICs. The security threats that are inherent to true 3D ICs, however, have not received much attention. We identify three potential security threats in 3D ICs: (1) the trustworthiness of vertical communication channel, (2) new hardware Trojan mechanisms, and (3) new side-channel attacks. To thwart reverse engineering attacks on the cross-plane communication (i.e. vertical communication channel), a NOC-SIP layer is proposed. The proposed NOC-SIP obfuscates the vertical communication within a 3D stack. Simulation results demonstrate that the proposed approach engages all of the routers as long as more than two pairs of I/O pads from different planes are in use. Alternatively, direct TSV connection method requires ten pairs of I/O pads from two planes to reach the same level of obfuscation as the proposed method. Thus, the proposed NOC-SIP makes it significantly more challenging for a reverse engineer to retrieve the vertical connectivity information. The proposed NOC-SIP was implemented with Verilog HDL and synthesized with a 65 nm technology. Synthesis results demonstrate that the proposed 3D router consumes approximately 1/5 of the area and power of a typical 2D router. This reduced overhead is achieved by the simplified single-plane and cross-plane ports in the 3D router.

7. REFERENCES

[1] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware Trojan Attacks: Threat Analysis and Countermeasures," *Proceedings of the IEEE*, Vol. 102, No. 8, pp. 1229–1247, 2014.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," *Advances in Cryptology—CRYPTO'99*, pp. 388–397. Springer, 1999.

[3] A. Moradi, M. T. M. Shalmani, and M. Salmasizadeh, "A generalized method of differential fault attack against AES cryptosystem," *Cryptographic Hardware and Embedded Systems-CHES 2006*. Springer, 2006, pp. 91–100.

[4] U. Guin, *et al.*, "Counterfeit integrated circuits: a rising threat in the global semiconductor supply chain," *Proceedings of the IEEE*, Vol. 102, No. 8, pp. 1207–1228, 2014.

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

[6] F. Courbon, P. Loubet-Moundi, J. J. Fournier, and A. Tria, "SEMBA: A SEM based acquisition technique for fast invasive Hardware Trojan detection," *Circuit Theory and Design (ECCTD), 2015 European Conference on*, pp. 1–4. IEEE, 2015.

[7] J. Zhang, H. Yu, and Q. Xu, "HTOutlier: Hardware Trojan detection with side-channel signature outlier identification," *Hardware-Oriented Security and Trust (HOST), 2012 IEEE International Symposium on*, pp. 55–58. IEEE, 2012.

[8] E. Prouff and M. Rivain, "Masking against side-channel attacks: A formal security proof," *Advances in Cryptology–EUROCRYPT 2013*. Springer, 2013, pp. 142–159.

[9] J. Blömer and J.-P. Seifert, "Fault based cryptanalysis of the advanced encryption standard (AES)," *Financial Cryptography*, pp. 162–181. Springer, 2003.

[10] H. Bar-El, *et al.*, "The sorcerer's apprentice guide to fault attacks," *Proceedings of the IEEE*, Vol. 94, No. 2, pp. 370–382, 2006.

[11] G. Di Natale, M. Doulcier, M.-L. Flottes, and B. Rouzeyre, "A reliable architecture for parallel implementations of the advanced encryption standard," *Journal of Electronic Testing*, Vol. 25, No. 4-5, pp. 269–278, 2009.

[12] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "Concurrent structure-independent fault detection schemes for the advanced encryption standard," *Computers, IEEE Transactions on*, Vol. 59, No. 5, pp. 608–622, 2010.

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

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] Y. Xie, C. Bao, and A. Srivastava, "Security-Aware Design Flow for 2.5 D IC Technology," *Proceedings of the 5th International Workshop on Trustworthy Embedded Devices*, pp. 31–38. ACM, 2015.

[19] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," *Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, ser. CRYPTO '96, pp. 104–113. London, UK, UK: Springer-Verlag, 1996. [Online]. Available: http://dl.acm.org/citation.cfm?id=646761.706156

[20] D. J. Bernstein, "Cache-timing attacks on AES," Tech. Rep., 2005.

[21] J. Valamehr, *et al.*, "A Qualitative Security Analysis of a New Class of 3-D Integrated Crypto Co-processors." *Cryptography and Security*, D. Naccache, Ed., pp. 364-382, 2012.

[22] S. Narasimhan, *et al.*, "Multiple-parameter side-channel analysis: A non-invasive hardware Trojan detection approach," *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on*, pp. 13–18. IEEE, 2010.

[23] C. Bao and A. Srivastava, "3D Integration: New opportunities in defense against cache-timing side-channel attacks," *Computer Design (ICCD), 2015 33rd IEEE International Conference on*, pp. 273-280, Oct 2015.

[24] J. Frey and Q. Yu, "Exploiting state obfuscation to detect hardware trojans in NoC network interfaces," *Circuits and Systems (MWSCAS), 2015 IEEE 58th International Midwest Symposium on*, pp. 1–4. IEEE, 2015.

[25] S. Saponara, *et al.*, "Design of an NoC Interface Macrocell with Hardware Support of Advanced Networking Functionalities," *Computer, IEEE Transactions on*, Vol. 63, No. 3, pp. 609-621, March 2014.