Detecting a Trojan Die in 3D Stacked Integrated Circuits

Soha Alhelaly[1], Jennifer Dworak[1], Theodore Manikas[1], Ping Gui[1], Kundan Nepal[2], and Alfred L. Crouch[3]
[1] Southern Methodist University, Dallas, TX, USA
[2] University of St. Thomas, St. Paul, MN, USA
[3] SiliconAid Solutions, Cedar Park, TX, USA

***Abstract*—While 3D integrated circuits provide many security advantages, one disadvantage is the insertion of a Trojan die into the stack. In this paper, we explore a technique to detect an extra die through delay analysis.**

Keywords—3D Integration; Security; Trojan; Delay; Test

I. INTRODUCTION

A 3D stacked integrated circuit (IC) can be manufactured by stacking multiple bare dies vertically and connecting them with through-silicon vias (TSVs). One expected benefit of these devices is an increase in performance in a very small form factor. Vertical connections between dies can be much shorter than the horizontal distance from one part of a die to another, and they may be many orders of magnitude shorter than the distance between different chips on a board. This can significantly increase the communication bandwidth between stacked dies in a package as opposed to chips on a board.

While 3D ICs are expected to have many advantages, they have proven to have disadvantages as well. Manufacturing and assembly can be difficult, and a single defective die in the stack will generally kill the entire stack, leading to low yield. Testing of 3D stacked ICs also introduces complications. Test patterns must be transmitted from the bottom of the stack to the die under test, and TSV connections between dies must be thoroughly tested as well. To address these issues, the IEEE P1838 working group is developing a standard for the transmission of test patterns through the stack [1]. Furthermore, multiple researchers have proposed ways of testing TSV connections [2]-[7].

3D stacked ICs also pose both advantages and disadvantages in the security domain [8]. For example, they inherently reduce access and observation of dies that are not directly connected to the pins at the bottom of the stack. This can enhance security because TSVs cannot be physically probed from outside of the stack. Thus, the ability of a third party to "snoop" communication between dies is much harder between dies in a 3D stack than between chips on a board. This inability to directly probe TSVs was discussed in [9], where a tester design for an FPGA in a 3D stack was proposed that could be used to send data to other layers of that stack. In [10], other researchers proposed a network-on-chip based 3D obfuscation method to prevent reverse engineering attacks on the vertical communication channel.

However, while the decreased observability of signals within a stack has security advantages, it poses security challenges as well. In [8], authors surveyed recent research work on 3D security, presented potential security issues, such as Trojans inserted in 3D ICs, and highlighted the need for future research efforts dedicated to unique issues of 3D IC security. The authors of [11]-[13], explained the new opportunity of inserting a Trojan layer into the stack of ICs which could be activated by timer or command.

One important 3D security issue is that an extra die could be added to the stack without the knowledge of the stack owner. Such a die could perform powerful attacks. For example, it could be placed between two dies and contain a memory to extract and save information from the data bus. An extra die could also consist of a hidden controller to interrupt chip operation or to destroy the chip by implementing malicious operations. Such a scenario is especially important to consider when third party assemblers combine dies from one or more companies into the stack. In such a case, the location of TSVs would be known a priori and could be used to construct an appropriate extra die.

In this paper, we assume that the attacker has the ability to add an extra die with the required TSV connections. However, he does not have access to the masks at the fab that would allow him to make changes on legitimate dies. Thus, only the presence of additional dies will be explored.

One possible method to detect such a Trojan involves X-raying the stack. However, X-raying a 3D stack is too time-consuming and expensive to be performed at a large scale except for critical and low-volume applications. Another possible approach to detect the extra die is to measure the power supply voltage drop experienced at the power supplying TSV's of an upper layer. In [14], the authors investigated the voltage drop for the worst case condition when all transistors switch simultaneously in the 3D stack by using electromagnetic (EM) and SPICE analysis. When the 3D stack has only one TSV for supplying voltage to the upper die in a 4 or 8 die stack, the voltage loss along the extra TSV's and microsolders between die is significant. However, the voltage difference between die levels off as one travels up the 3D stack, and decreases significantly if extra TSV's are also used

This paper was supported in part by NSF grant CCF-1061164.

978-1-5090-5902-7/17/$31.00 ©2017 IEEE

to transfer power and gnd. Another approach is to use Trojan detection techniques that are based on side-channel analysis. However, using such techniques in 3D ICs are more difficult because of the stacking structure of multiple dies on top of each other, high device density nature of 3D chips, and fabrication process variations of the 3D ICs [8].

Adding an extra die to the stack is likely to affect the communication delay between layers. Thus, detecting this added delay is one potential approach to finding such a die. Such delay could be found automatically with no additional testing effort if the communication between layers was sufficiently fast and had little slack. In that case, placing an extra die between layers could lead to all of the corresponding interconnect tests or even the functional communication failing outright. However, when margins are high to maintain yield or when high speed communication is not needed, then it is possible that an extra die between layers may not be detected by normal testing.

In this paper, we investigate this issue. In particular, we use simple TSV models previously published by other researchers [15] to estimate the delay as additional dies are added to the stack. We show that ring oscillator (RO) based test structures based on the bottom of the stack and incorporating different layers can be used to detect the extra delay and identify and locate the presence of an extra die. However, when process variation is included, the differences between a die in a stack with a Trojan can be harder to detect with this structure. An alternative ring oscillator-based test structure that incorporates fewer dies will then be investigated. We will show that in the presence of process variations, such a structure may allow the delay impact of the extra die to be more readily apparent.

The rest of this paper is organized as follows. Section II discusses the test instrument we are using to measure delay and detect potential extra die. Section III presents the TSV structure and delay model. Section IV presents the measurement procedure. Section V discusses our simulation results. Section VI concludes the paper and discusses future work.

II. RING OSCILLATOR BASED TEST INSTRUMENT

In this paper, we propose a detection technique that can measure the propagation delay across dies with the ability to detect the location of the extra die. It is assumed that placing extra dies in the propagation path will increase the propagation delay of signals sufficiently to allow that die to be detected. The goal of this paper is to determine if that assumption is true in an ideal case under various scenarios and in the presence of process variations.

Ring oscillators are commonly used to measure delays because the period of oscillation is directly related to the delay through the closed path. As a result, they have been inserted even in 2D devices to help quantify process variations in different areas of a chip as well as to sense changes in voltage, temperature, or aging. Ring oscillators have also been used in 3D stacked devices to characterize TSVs. For example, in [7], a ring oscillator was used to detect defective TSVs, and a Built-In-Self-Test (BIST) 3D ring oscillator was proposed in [15] for testing the stacked 3D IC.

We utilize the ring oscillator design similar to the one proposed in [15] to measure the extra delay that may appear between dies. In particular, we use a 3D ring oscillator test structure consisting of 13 stages. The ring oscillator is modeled in SPICE with 65-nm technology CMOS. The authors of [16] note that ring oscillators suffer from frequency deviation caused by Process-Voltage-Temperature (PVT) variations and poor jitter performance. They recommend using a voltage-controlled oscillator (VCO) to have a better performance and to oscillate at a particular frequency, instead of using a free-running ring oscillator.

Thus, the current-starved cells proposed by [15] provide more flexibility and sensitivity in the control of both current and voltage, which directly impacts the oscillation frequency [17] [15]. Assuming that the delay introduced by the routing between inverters is negligible, a 3D ring oscillator's delay period depends on three factors: the delays of the inverters, the delays of the TSVs that connect the layers, and the delays induced by the driver circuitry for the TSVs. The overall delay associated with the TSVs is dominated by the TSVs' capacitances and the drivers' resistances [18] [19]. In this paper, we propose a technique to observe the oscillation period of the 3D ring oscillator to detect abnormal delay caused by the inserted Trojan die.

The current-starved cell simulated for this paper is shown schematically in Figure 1 (a) and consists of four MOSFETs (M1–M4) [17]. MOSFETs Ml and M4 serve as current sources to limit the current that may be drawn by the inverter. MOSFETs M2 and M3 serve as an inverter, which is starved for current. The MOSFETs M5 and M6 in Figure 1 (b) are controlled by the voltage (Vctrl). The control voltage is used in Figure 1 (b) to adjust the current that flows in M5 and M6. The current through M5 and M6 is mirrored by each current source stage. Therefore, the change in the control voltage (Vctrl) makes a change in the inverter currents, and directly impacts the delay [17].

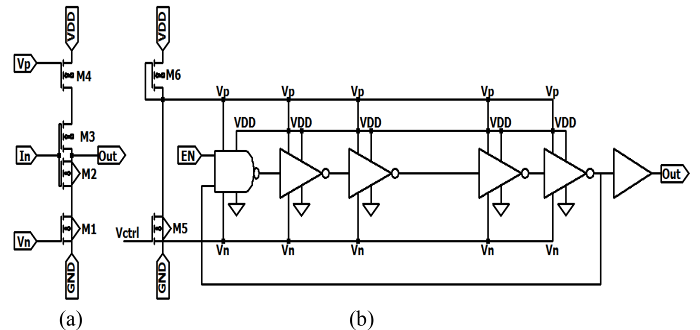

Fig. 1. Circuit schematic of current-starved ring oscillator. (a) current-starved cell. (b) 2D current-starved ring oscillator [17].

Figure 2 shows the circuit schematic of the 3D ring oscillator using thirteen current-starved delay cells. The delay cells are modeled as being distributed across two dies for each ring oscillator. The bottom die has a NAND gate, five inverters, and the output buffer, while the top die has seven inverters. Modeling of the TSV portion of the figure is explained in the next section. The rectangles correspond to TSVs that connect signals in both dies. The initial proposed 3D ring oscillator test structure for detecting an extra die

measures the signal delay from the bottom die to each die in the 3D stack. For instance, if the 3D IC consists of four dies, we should have three ring oscillators. The first ring oscillator measures the delay from die 1 at the bottom to die 2. The second ring oscillator measures the delay from die 1 at the bottom to die 3. Finally, third ring oscillator measures the delay from die 1 at the bottom to the top die in the stack. A drawing of how these three ring oscillators connect different layers of the stack is shown in Figure 3 (a).

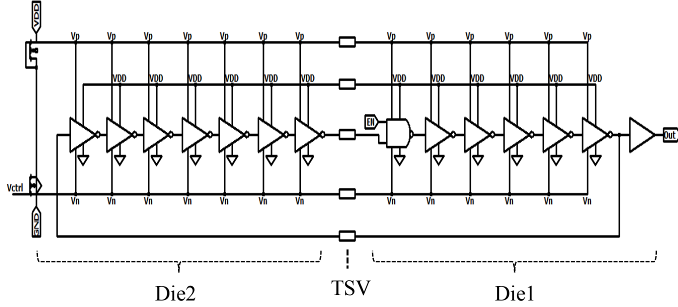

Fig. 2. Circuit schematic of 13 stages current-starved 3D ring oscillator in two dies.

This approach has the advantage that all RO testing can be controlled by the base die, which can be designed specifically to implement these and other security functions. It also naturally provides multiple test ring oscillator structures that can be used to distinguish between an extra die and a defective TSV.

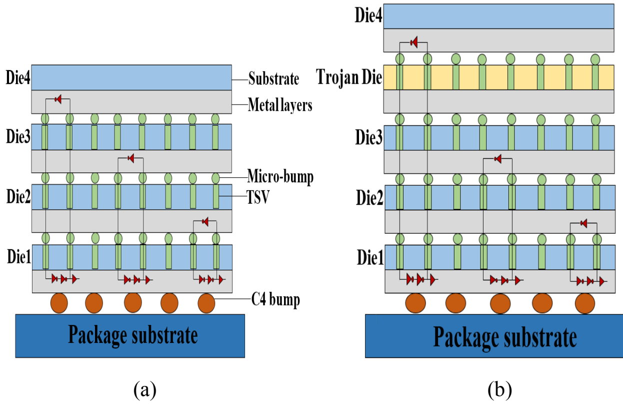

Fig. 3. Circuit 3D ring oscillators tests. (a) Test structure without a Trojan die. (b) Test structure with a Trojan die between the Die 3 and Die 4.

A possible disadvantage of this approach is that coordination is required between die IP owners to provide the appropriate RO connections and gates on the corresponding dies. However, this issue may be addressed by locating all counters and control on the bottom die. Space may also need to be allocated for pass-through TSVs for the test structures by all dies if the stacking order is not known a priori, even if it means some of them are not ultimately used.

III. TSV STRUCTURE AND RC MODEL

The Trojan-free design configuration used in our simulations is composed of face up stacked die. Copper is used as the conductor material for the TSVs in our analysis, and silicon dioxide (SiO2) is assumed to be the insulator around the copper conductor. The TSVs used are cylindrical and have a circular cross-section.

When the TSV is used as a channel for transmitting a digital signal, SPICE simulation reveals that the most dominant factor of the TSV's delay is the TSV capacitance; the effect of the TSV resistance is small, and the effects of inductance and conductance can be almost ignored [15]. According to multiple studies, the TSV delay is dominated by TSV's capacitance and the driver's resistance [15] [18]. Thus, we utilize the simpler RC model used in [15] [20] to represent the TSV parameters in the SPICE simulation. In these previous studies, the effect of the micro-bump was also combined with that of TSV itself [15] [21].

To model the driver, we use a TSV driver's equivalent on-resistance (Rdriver) which is usually in the range of several kiloohms for 65-nm CMOS technology [18]. However, the driver capacitance (Cdriver) is small and measures only a few femtofarads, as described in [18]. Thus, Figure 4 shows the simplified equivalent circuit of the TSV used for the analysis of the proposed test procedure [15]. Other models, such as the Pi and T model were also explored without any significant changes in the results in this paper.

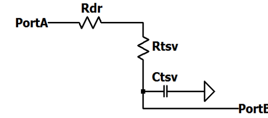

Fig. 4. Simplified RC-based delay model for the TSV with a driver for the experiments [15].

For a cylindrical copper-filled TSV, we estimate the resistance and capacitance using the following equations [20]:

$$R_{TSV} = \frac{\rho_m h}{\pi {r_{via}}^2} \tag{1}$$

$$C_{TSV} = \frac{2\pi\varepsilon_r\varepsilon_0 h}{\ln((r_{via}+t)/r_{via})} \tag{2}$$

where h is the height of the TSV, r_{via} is the TSV radius, and ρ_m is the resistivity of Copper. ε_r and ε_0 are the relative SiO2 permittivity and empty space permittivity, respectively. t is the dielectric (SiO2) thickness. TSV parameters such as height, width, and pitch are obtained from the International Technology Roadmap for Semiconductors [22]. For example, by using the minimum height and width, the TSV would have the following physical parameters: a height of 30um, a width of 2.5um, and a thickness of 1um. These parameters were chosen to minimize the expected TSV delay in our analysis. The estimated resistance and capacitance are about 0.1027ohms and 11.0629fF, respectively. For the driver's resistance, we use 5KΩ in our simulations.

IV. MEASUREMENT PROCEDURE

Although extra delay in inter-die communications in the stack could be due to an extra Trojan die inserted in the stack, it could also be due to a simple defect in a TSV or ring

oscillator gate. As a result, the proposed approach shown in Figure 3 (a) allows multiple ring oscillators to be used to test for Trojans hidden in the lower layer of the stack. If the 3D circuit consists of n dies, we should have n-1 ring oscillators. Each ring oscillator is used to measure the roundtrip delay from the bottom die to each die in the stack.

For example, a Trojan extra die inserted between dies 1 and 2 should add a certain amount of extra delay to all three ring oscillators. This will help to distinguish the presence of an extra die from a simple defect in a TSV, route, or gate. Similarly, a die inserted between dies 2 and 3 should add delay to two ring oscillators. Of course, an extra die between dies 3 and 4 will add delay to only one ring oscillator. Such delay could also be due to a defective TSV or gate. To distinguish this, an additional ring oscillator from the bottom to the top of the stack could be inserted, if desired. Thus, the proposed method can be used to not only identify suspect stacks, but to determine the location of the extra die within the stack itself while accounting for potential defects in the test structures.

The test structure consists of three elements:

- A 3D ring oscillator, which is used to measure the delay across the dies.
- A frequency counter that is fed by the 3D ring oscillator and that is needed to determine the measured oscillation frequency and compare it with "golden" reference values over some reference period.
- Control circuitry that can be accessed through the test network (e.g. IEEE 1687) and used to enable the test and obtain the results.

The area overhead introduced by the proposed approach can be reduced by using some of the existing TSVs in the 3D stack for the test purpose. In addition, the area overhead of the inverters and the counters is small.

There are several steps to perform the test analysis for Trojan detection. Step 1 enables each RO in turn for a predetermined amount of time. The count obtained by the associated counter corresponds to a surrogate measure of the delay: Test1, Test2,…Test(n-1). Step 2 calculates the counter differences between each successive ring oscillator (ΔD1, ΔD2, and ΔD(n-1)) to get a measurement proportional to the delay caused by traveling to the next die. For example, ΔD(n-1) is obtained by calculating:

$$\Delta D(n-1) = Test(n-1) - Test(n-2) \quad (3)$$

Note that this differential is proportional to approximately four times the TSV delay of traversing to the next die because the full circuit path of the RO traverses each intermediate die in its path twice (going up and going down) in one half period.

Then, Step 3 calculates the percentage change (TP1, TP2, TP(n-1)) between the obtained delay differences of the tests (ΔD(1), ΔD(2),…ΔD(n-1)) and the golden reference values (ΔDref(1), ΔDref(2),…ΔDref(n-1)) by using:

$$TP(n-1) = \left(\frac{\Delta D(n-1) - \Delta Dref(n-1)}{\Delta Dref(n-1)}\right) \times 100\% \quad (4)$$

Here ΔDref corresponds to the expected additional delay when no extra Trojan die is present. It may be obtained by accurate simulation or preferably by measurement of 3D stacks that have been proven not to contain any Trojan die (e.g. by taking the measurement and then carefully disassembling the stack to check for tampering or incorrect assembly). The test percentage change TP(n-1) is obtained by comparing ΔD(n-1) with the reference value ΔDref(n-1).

In Step 4, we compare the results from multiple ring oscillators to try to determine if an extra delay is likely due to a Trojan die or a simple delay defect. If the same delays are seen in multiple ROs, then the delay is more likely to be due to a Trojan die, and the location of the Trojan can be pinpointed. As already noted, to more accurately diagnose a Trojan near the top of the stack, additional test ROs could be included.

V. SIMULATION RESULTS

To study the impact of the TSVs on the ring oscillator frequency, we compared the frequency of the 13-stage 3D ring oscillator that connects two dies with a 13-stage 2D ring oscillator entirely contained a single die when the control voltage is 1V. In both cases, a load corresponding to the frequency counter was included. The simulated results show how the TSVs affect the frequency of the 3D ring oscillator, as shown Table 1.

TABLE I. OSCILLATION FREQUENCY OF THE 13-STAGE 2D AND 3D RING OSCILLATOR

13-stage 2D ring oscillator	13-stage 3D ring oscillator (two dies)
1.71 GHz	1.27 GHz

A. *Detecting an Extra Die between Die 3 and Die 4*

To evaluate the proposed test technique, the Trojan-free design and the compromised 3D stack were simulated using SPICE with 65nm CMOS technology, using the parameters specified in Section 3. The oscillation frequency is determined by setting Vctrl=VDD=1V. The experiments were performed for a 3D IC that consists of four face up dies. Therefore, we needed three ring oscillators, such as those shown in Figure 3 (a). For the compromised stack, we inserted an extra die between die 3 and die 4 in the CUT as shown in Figure 3 (b). Furthermore, we assumed the worst case that the additional circuits in the Trojan die are not connected to the test structure. Table 2 shows the data derived for the three ring oscillators. The simulated results indicate that the Trojan die is detected with this test structure. Column 1 is the test number and corresponds to a ring oscillator, while columns 2–3 show the timing measurements of the Trojan-free design. Note that in this simulation, instead of obtaining counts over a particular time period, the frequency of oscillation was extracted from SPICE simulation. This was inverted to obtain the period. Thus, the value in Column 2 corresponds to the oscillation period of the ring oscillator and the value in Column 3 corresponds to the difference in oscillation period between successive ring oscillators. Columns 4–5 show the same calculations for the 3D stack under test, where an extra die has been inserted between dies 3 and 4. Column 6 shows the percentage increase of the ΔD value between the Trojan-free reference design and the stack containing the Trojan die. A sufficiently large increase (or repeated increases when the extra

Trojan die is located lower in the stack) could indicate the existence of an extra Trojan die.

In this case, the presence of an extra Trojan die causes a 93% increase in the ΔD value between dies 3 and 4 over the value expected when no extra die is present in the stack.

TABLE II. TROJAN DIE BETWEEN DIE 3 AND DIE 4 AND VCTRL=1V

Test	**Measurement for Trojan-free stack (Reference values)**		**Measurement for a stack with a Trojan die**		**Result**
	Delay (ps)	***ΔDref (ps)***	***Delay (ps)***	***ΔD (ps)***	***Percentage change between ΔD and ΔDref***
1	787.40	787.40	787.40	787.40	(No difference)
2	938.97	151.57	938.97	151.57	(No difference)
3	1069.52	130.55	1190.48	251.51	93% (the delay is increased)

B. *The Impact of Process Variations of the Ability to Detect an Extra Die*

In the previous experiments, we simulated our detection method assuming that there were no process variations. However, significant process variations could make it more difficult to clearly identify delay differences due to an extra Trojan die instead of natural variation. To investigate this, we used Monte Carlo simulation to mimic the process variation. We used a Gaussian distribution for the variation by using SPICE with 65nm technology over 10,000 samples to reflect variation. The Monte Carlo analysis was done by giving a tolerance interval to five parameters, including TSV capacitance, TSV resistance, driver resistance, transistor length, and transistor width (including variation on each MOSFET of the ring oscillator gates and the current-starved cells). All parameters were varied 10% (1σ) from the nominal values simultaneously.

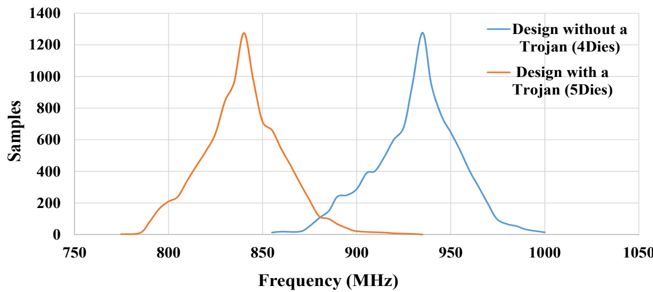

Fig. 5. Monte Carlo simulation of 10,000 circuit samples.

We performed the Monte Carlo simulation for a 3D ring oscillator that consists of four dies without a Trojan and the same 3D ring oscillator with a Trojan die between die 3 and die 4 as shown in Figure 3 (b). Then, we compared the frequency of the RO that has a Trojan with the same RO in the Trojan-free stack. Unfortunately, process variations in the test components produce significant natural variation in the frequencies of the ring oscillators even when no extra dies are present. Figure 5 shows the probability distribution of frequencies for both the Trojan-free and Trojan cases. Even though the average difference in oscillation frequency is approximately 95 MHz, there is still significant overlap in the distributions that might cause missed Trojan dies or many false alarms depending on what threshold value is chosen to indicate a potential extra die.

C. *Modifying the Test Structure to Increase the Impact of the Extra Die*

As we see from the simulation results in Table 2, the increase in oscillation period does not appear to be constant as we add more dies to the stack. In a stack without a Trojan, the increase in oscillation period when three dies are included in the RO instead of two is equal to 151.57 ps (i.e. 938.97 ps - 787.40 ps). In contrast, the increase in oscillation period when four dies are included in the RO instead of three is equal to 130.55 ps (i.e. 1069.52 ps - 938.97 ps). Thus, one way to magnify the impact of an extra die could be to use smaller ROs that encompass fewer dies in the stack. This leads to an alternative test structure shown in Figure 6 (a), where each test RO only encompasses two legitimate dies.

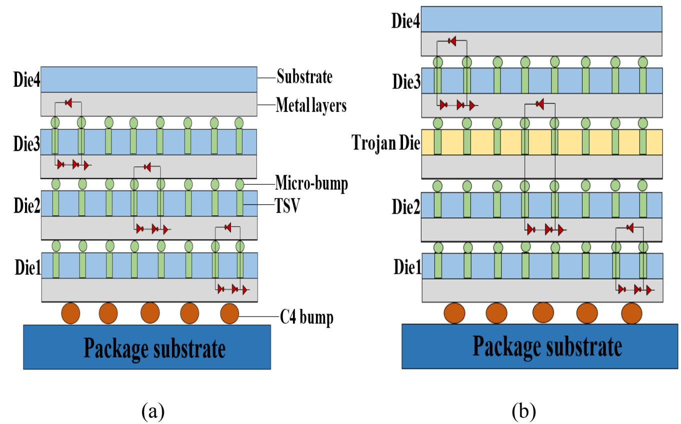

Fig. 6. Test structure with 3D ring oscillators encompassing two dies. (a) Trojan-free stack. (b) Test structure with a Trojan die.

To explore the impact of the process variations on the alternative structure, we performed a Monte Carlo simulation for a 3D ring oscillator without a Trojan (2 dies) and the same 3D ring oscillator with a Trojan die between them (3 dies) as shown in Figure 6 (b). The results of Monte Carlo simulation of 10,000 circuit samples with the same 10% (1σ) variation show that the two distributions are now distinct as shown in Figure 7.

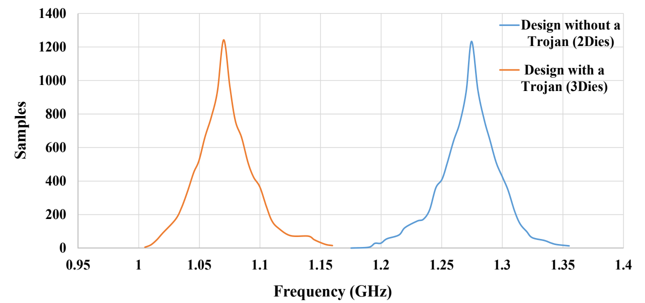

Fig. 7. Monte Carlo simulation of 10,000 circuit samples.

This alternative structure has some other advantages as well. Less coordination and planning among die IP owners is

needed to leave space for the test TSVs because specific TSV locations could be standardized and allocated for the test structure that would be the same on every die in the stack. Of course, increased standardization also makes it easier for an attacker to make changes to help hide an extra die at assembly (e.g. by changing the sizes of the TSVs). Furthermore, the ability to extract the counter data from each die must be provided because all of the counters are not located on the base die. This is not likely to be a significant problem. For example, the counter results could be accessed as normal embedded instruments through an IEEE 1687 network on the chip [23], where the IEEE 1687 network is accessed through the IEEE P1838 test elevator interface. Finally, to prevent defective ROs or TSVs from identifying stacks as containing extra Trojan dies, two or more RO test structures per level could be used and their results compared to make the determination.

VI. CONCLUSION

In this paper, we have introduced two approaches to detect an extra die between two legitimate dies in a 3D stack using 3D ring oscillators. In some cases, the delay introduced by an extra die may be detectable by normal connectivity tests between dies when there are small margins and very low process variations. However, if the slack of the inter-die connections is large to help maintain yield and handle process variations, a Trojan die could be missed without explicit testing. To best handle process variations, the proposed test structure of 3D ring oscillators encompassing two dies should be used. With this structure, we can detect and locate an extra die between stacked die with the variation of 10% (1σ) from the nominal values.

In future work, we will further characterize the RO based test structures for the detection an extra die under other conditions. For example, other amounts of process variations and temperature variations can be included. Methods that an attacker might use to modify the stack to avoid detection, such as by varying the size of the TSVs and dielectric thickness to better hide the added delay, will be considered. Future work will also consider the possibility that a Trojan die is placed on the top and bottom of a stack instead of between layers. Furthermore, attackers could theoretically include the ring oscillator's inverters in the Trojan die itself and complete the chain to reduce or eliminate the effect of the extra die on RO measurements. We are developing countermeasures to this as well. Finally, there may be alternate ways of designing and grouping ring oscillators, and these will be investigated in a later paper.

REFERENCES

[1] "IEEE 3D-Test Working Group (3DT-WG)," Aug. 2016.

[2] C. C. Chi, C. W. Wu, M. J. Wang, and H. C. Lin, "3D-IC interconnect test, diagnosis, and repair," *VLSI Test Symp. VTS 2013 IEEE 31st*, pp. 1–6, Apr. 2013.

[3] C. Wang *et al.*, "Bist methodology architecture and circuits for pre-bond tsv testing in 3d stacking ic systems," *IEEE Trans. Circuits Syst. Regul. Pap.*, vol. 62, pp. 139–148, Jan. 2015.

[4] L.-C. Li, W.-H. Hsu, K.-J. Lee, and C.-L. Hsu, "An efficient 3d-ic on-chip test framework to embed tsv testing in memory bist," *20th Asia S. Pac. Des. Autom. Conf.*, pp. 520–525, Jan. 2015.

[5] P. Y. Chen, C. W. Wu, and D. M. Kwai, "On-chip testing of blind and open-sleeve TSVs for 3D IC before bonding," *2010 28th VLSI Test Symp. VTS*, pp. 263–268, Apr. 2010.

[6] W. H. Hsu, M. A. Kochte, and K. J. Lee, "3d-ic test architecture for tsvs with different impact ranges of crosstalk faults," *2016 Int. Symp. VLSI Des. Autom. Test VLSI-DAT*, pp. 1–4, Apr. 2016.

[7] Y. Fkih, P. Vivet, B. Rouzeyre, M. l. Flottes, and G. Di Natale, "A 3D IC BIST for pre-bond test of TSVs using Ring Oscillators," *New Circuits Syst. Conf. NEWCAS 2013 IEEE 11th Int.*, pp. 1–4, Jun. 2013.

[8] Y. Xie, C. Bao, C. Serafy, T. Lu, A. Srivastava, and M. Tehranipoor, "Security and Vulnerability Implications of 3D ICs," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 2, no. 2, pp. 108–122, Jun. 2016.

[9] Y. Sun, "Using an FPGA in a 3D Stacked IC to Prevent LSIB Bitstream Snooping," Master, Southern Methodist University, Dallas, Texas, 2013.

[10] J. Dofe, Q. Yu, H. Wang, and E. Salman, "Hardware Security Threats and Potential Countermeasures in Emerging 3D ICs," *2016 Int. Gt. Lakes Symp. VLSI GLSVLSI*, pp. 69–74, May 2016.

[11] J. Ellis, "A Call to Action on 3D IC Security," *Chip Security*, 01-Mar-2012. [Online]. Available: http://chipsecurity.org/2012/03/a-call-to-action/.

[12] E. Worthman, "Designing For Security," *Semiconductor Engineering*, 08-Jan-2015. [Online]. Available: http://semiengineering.com/designing-for-security-2/.

[13] K. XIAO, D. FORTE, Y. JIN, R. KARRI, S. BHUNIA, and M. TEHRANIPOOR, "Hardware Trojans: Lessons Learned after One Decade of Research," vol. Volume 22, no. Issue 1, Nov. 2016.

[14] Z. Xu, J. Q. Lu, B. C. Webb, and J. U. Knickerbocker, "Electromagnetic-SPICE modeling and analysis of 3D power network," *2011 IEEE 61st Electron. Compon. Technol. Conf. ECTC*, pp. 2171–2178, May 2011.

[15] C. Jin *et al.*, "Built-in-Self-Test-Stacked 3-D Ring Oscillator Based on Through Silicon Vias," *IEEE Trans. Compon. Packag. Manuf. Technol.*, vol. 5, no. 2, pp. 217–224, Feb. 2015.

[16] A. Hajimiri, S. Limotyrakis, and T. H. Lee, "Jitter and Phase Noise in Ring Oscillators," *IEEE J. Solid-State Circuits*, vol. 34, no. 6, pp. 790–804, Jun. 1999.

[17] J. Baker, *CMOS: Circuit Design, Layout, and Simulation*, Third Edition. Hoboken, New Jersey, USA: John Wiley & Sons, Inc, 2010.

[18] J. W. You *et al.*, "In-Situ Method for TSV Delay Testing and Characterization Using Input Sensitivity Analysis," *IEEE Trans. Very Large Scale Integr. VLSI Syst.*, vol. 21, no. 3, pp. 443–453, Mar. 2013.

[19] M. A. Ahmed and M. Chrzanowska-Jeske, "Delay and Power Optimization with TSV-aware 3D Floorplanning," *Fifteenth Int. Symp. Qual. Electron. Des.*, pp. 189–196, Mar. 2014.

[20] I. Savidis, S. M. Alam, A. Jain, S. Pozder, R. E. Jones, and R. Chatterjee, "Electrical modeling and characterization of through-silicon vias (TSVs) for 3-D integrated circuits," *Microelectron. J.*, vol. 41, no. 1, pp. 9–16, Jan. 2010.

[21] N. Niioka *et al.*, "Impact of On-Chip Interconnects on Vertical Signal Propagation in 3D ICs," *Circuits Syst. APCCAS 2014 IEEE Asia Pac. Conf. On*, pp. 607–610, Nov. 2014.

[22] "INTERNATIONAL TECHNOLOGY ROADMAP FOR SEMICONDUCTORS (INTERCONNECT)," 2.0, 2015.

[23] "1687-IEEE Standard for Access and Control of Instrumentation Embedded within a Semiconductor Device," IEEE Std 1687-2014, pp. 1–283, 2014.