IEEE TRANSACTIONS ON
EMERGING TOPICS
IN COMPUTING

Received 9 July 2019; revised 18 March 2020; accepted 19 March 2020.
Date of publication 2 April 2020; date of current version 4 June 2021.

Digital Object Identifier 10.1109/TETC.2020.2984162

3D Ring Oscillator Based Test Structures to Detect a Trojan Die in a 3D Die Stack in the Presence of Process Variations

SOHA ALHELALY, JENNIFER DWORAK, (Member, IEEE), KUNDAN NEPAL, (Senior Member, IEEE), THEODORE MANIKAS, (Senior Member, IEEE), PING GUI, (Senior Member, IEEE), AND ALFRED L. CROUCH, (Senior Member, IEEE)

S. Alhelaly is with Saudi Electronic University, Riyadh 13323, Saudi Arabia
J. Dworak, T. Manikas, and P. Gui are with the Southern Methodist University, Dallas TX 75205, USA
K. Nepal is with the University of St Thomas, St Paul MN 55105, USA
A.L. Crouch is with the Amida Technology Solutions, Austin TX 78728, USA
CORRESPONDING AUTHOR: S. ALHELALY (s.alhelaly@seu.edu.sa)

ABSTRACT 3D integrated circuits introduce both advantages and disadvantages for security. Among the disadvantages unique to 3D is the potential insertion of a Trojan die into the stack between two legitimate dies. Such a die could be used to snoop information traveling between dies, alter the data, or otherwise interfere with stack operation. In this article, we explore the use of in-stack circuitry and various testing procedures to detect an extra die through delay analysis even in the presence of process variations. Then, we explore the performance of these techniques when the attacker modifies some of the TSVs' characteristics to avoid detection. Our simulation results show that the proposed techniques can detect the Trojan die in a 3D stack, especially when the test structure that incorporates multiple TSVs between two dies is used.

INDEX TERMS 3D integration, TSV, security, Trojan, extra die, 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). While such 3D stacked ICs are likely to have many advantages related to power and performance, they introduce important security challenges regarding the potential introduction of Trojan dies into the stack—especially at packaging when the stack is assembled. The ability to devote an entire die to Trojan behavior could allow particularly powerful attacks. This possibility must be recognized by test and security engineers at the stack, board, and system level, and reliable methods for Trojan die detection that can be applied at each level are needed. This paper aims to provide a detailed analysis of such a test structure that will enable Trojan die detection.

The possibility of a Trojan being present in 3D stacks has been previously discussed by other researchers, but without the needed solutions for Trojan die detection. For example, in [1], the authors surveyed recent research on 3D security. They presented potential 3D security issues as compared to their 2D counterparts, including the possibility of Trojans and counterfeits being included in a 3D stack, and they highlighted the need for future research efforts dedicated to the unique issues of 3D IC security. However, they did not explicitly consider the possibility of an extra die being inserted into the stack for Trojan purposes.

In contrast, the authors of [2], [3], [4], [5], have previously discussed the potential for an attacker to insert a Trojan layer into the stack of ICs, where the Trojan die could be activated by a timer or a command. However, they did not investigate any solutions for the problem. Instead, they demonstrated the need for future efforts dedicated to studying the Trojan die issue in 3D ICs. To the best of our knowledge, our work is the first to explore solutions for the detection of a Trojan die inserted between legitimate layers of a 3D stack.

One possible way of detecting extra dies in the stack is through added delay. Two dies that are intended to be adjacent would be expected to experience more delay if an additional die were inserted between them. Such delay could possibly be found during normal delay testing of inter-die interconnects if the designed slack were sufficiently small and the process variations are low. Multiple researchers have

2168-6750 © 2020 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: SOUTHERN METHODIST UNIV. Downloaded on June 04,2021 at 22:11:09 UTC from IEEE Xplore. Restrictions apply.

IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING

proposed ways of testing TSV connections [6], [7], [8], [9], [10], [11].

However, depending upon the stack design and expected tolerances, normal delay testing may not necessarily lead to automatically detecting a Trojan die—especially in the presence of significant process variations. In particular, it is hard to attain high yield in a 3D stack because there are so many locations (including many dies and interconnects) where something can go wrong, and 3D stacks cannot be repaired by de-soldering and replacing a bad die as can occur with a bad chip on a board. Furthermore, the cost of discarding a stack that doesn't meet specifications can be very high because all the dies in the stack must be discarded simultaneously. Thus, in many cases, interconnects between dies are likely to be designed with significant slack to maintain yield. An extra die might not be detected under such conditions, especially if the assembler is able to alter the TSV characteristics to reduce the additional delay.

Thus, there is a need to investigate test techniques to detect the extra delay that arises due to a presence of a Trojan die and whether such additional delay can still be detected even in the presence of process variations. It is also necessary to determine what circumvention approaches an attacker may employ to avoid detection, and then develop design techniques that make these approaches less effective.

In [12], we published our initial work on Trojan die detection. In particular, we used simple TSV models previously published by other researchers [13] to estimate the increase in delay through TSVs as additional dies are added to the stack and explored the ability of a ring oscillator (RO) based test structure to detect this added delay. We showed that the proposed test structure of 3D ring oscillators encompassing two dies can detect and locate an extra die between stacked dies with the variation of 10% from the nominal values.

In this article, we expand on the work described in [12]. Specifically, we describe the following investigations:

- We explore the potential ability of an attacker to modify the TSV characteristics such as height and diameter. We show that the test structure that incorporates two dies could miss detecting a Trojan die if an attacker succeeds in placing a Trojan die with smaller TSVs than the one used in the adjacent good dies in the stack, especially with the presence of process variation.
- We also explore the degree to which TSV dielectric thickness modifications made by an attacker may impact our ability to detect an extra die with delay measurements. We show that there is a possibility of many false alarms or missed Trojan dies with the presence of the process variation.
- We explore the potential ability of an attacker to alter the test structure and include the ring oscillator's inverters in the Trojan die itself to avoid detection. Then, we characterize the test structures and their ability to detect the extra Trojan die even when the attacker alters the test structure.
- We propose additional test structures that incorporate multiple TSVs connected serially between two dies to magnify the impact of a Trojan die and to increase the probability of detecting it even when an attacker tries to avoid detection. We show that these test structures are more promising to detect such a Trojan die even when an attacker attempts to modify the TSVs' parasitics or to alter the test structure, and even in the presence of process variation.

The rest of this article is organized as follows. Section II describes why Trojan dies could significantly impact security in addition to some of our assumptions about the ability of an attacker to insert a Trojan die. Section III presents preliminary analysis of potential approaches for detecting a Trojan die in a 3D stack and describes previous work in detecting such a Trojan die. Section IV discusses some of the attacker's responses to avoid detection. Section V proposes alternative test structures that incorporate multiple TSVs, and measures the efficiency of these techniques with the attacker's responses. Section VI concludes the paper.

II. HARDWARE TROJANS IN 3D ICS

The insertion of a Trojan die could lead to powerful attacks. For example, it could be placed between two dies to extract information from the data bus and save it in memory for later access. An extra die could also consist of a hidden controller intended 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 Trojan die. Thus, in this article, we assume that the attacker has the ability to add an extra die with the required TSV connections. However, he/she does not have access to the masks at the fab that would allow him/her to make changes on legitimate dies. As a result, only the presence of additional dies will be explored.

Note that adding a Trojan die to the stack may be easier in many ways than inserting a Trojan into an otherwise legitimate die. It does not require reverse engineering the original die(s) in the stack and finding small areas where the Trojan can be placed without affecting the operation of the original chip. For many attacks, the attacker merely needs to know the location and functionality of the TSVs to create a die that can maliciously steal or control data passing between dies (e.g., on a data bus). The attacker can also provide much more sophisticated Trojan behavior in an extra die that cannot be discovered by simply testing individual dies before stacking. Such a die can be "off" or in "low power mode" most of the time and turn on only under specific conditions. Furthermore, in many cases, such a die can be made cheaply, using large feature sizes in an old technology node when high performance behavior is not needed.

III. DETECTING A TROJAN DIE

There are multiple potential approaches for detecting an extra Trojan die between layers in a 3D stacked IC. Unfortunately, many of these approaches present challenges that make them

Authorized licensed use limited to: SOUTHERN METHODIST UNIV. Downloaded on June 04,2021 at 22:11:09 UTC from IEEE Xplore. Restrictions apply.

unsuitable in many environments. For example, 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 [2]. We also examined the possibility that an extra die might be found by weighing the stack. To work, this would require very accurate measurements and low natural variation between chips. To investigate this possibility, we weighed thirty identical IC packages using a precision balance that weighs in increments of as small as 0.0001 grams. We found that the weights measured for the 30 different chips varied more than the expected weight that would be added by an extra die. Thus, the natural variation in the measurements likely make this a difficult, if not impossible approach to detecting a Trojan die in the stack.

Another method that might not be practical to detect the Trojan die in a stack is measuring the height of the 3D IC package. An attacker might be able to use techniques to hide a Trojan die that is designed to be especially thin within a stack—thus keeping the overall package height similar to the original stacked height. The percentage change in height will also be less in a larger stack [14]. In [15], the authors have stated that by using various techniques, such as thin backgrind wafer technology, a triple-stacked die still meets the maximum thickness ceiling required as in the original package of the two stacked dies. Therefore, a Trojan die might not increase the package height if the attacker uses such techniques to hide it. Finally, the height of a die is generally very small, on the order of tens of microns. The natural variation in the height of a 3D package is likely to mask the change in the height of the stack due to a Trojan– especially without the use of expensive test equipment.

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. Although the authors of [16] were not trying to detect Trojan dies, they used electromagnetic (EM) and SPICE analysis to investigate the voltage drop when all transistors switch simultaneously in the 3D stack. 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 TSVs and microsolders between dies is significant. However, the voltage difference between dies levels off as one travels up the 3D stack, and decreases significantly if additional TSVs are also used to transfer power and ground.

An alternative approach involves taking advantage of the fact that adding an extra die to the stack is likely to affect the communication delay between layers separated by the Trojan 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 pass/fail testing.

A. INITIAL TEST STRUCTURE ANALYSIS

1) DETECTING A TROJAN DIE IN A 3D STACK

In [12], we published our initial work on extra Trojan die detection. We proposed 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 proposed approach was to determine if that assumption is true in an ideal case under various scenarios and in the presence of process variations. We used an RC model from [13], [17] to represent the TSV parameters in the SPICE simulation and to estimate the increase in delay through TSVs as additional dies were added to the stack. We also explored the ability of a ring oscillator (RO) based test structure to detect this added delay. For a cylindrical copper-filled TSV, we estimated the resistance and capacitance using the equations from [17]. TSV parameters such as height, diameter, and pitch were obtained from the International Technology Roadmap for Semiconductors [18]. (Data were also collected for other TSV models, such as the π and T-models, but no significant changes that would affect the results in this paper were found).

We utilized a ring oscillator design consisting of 13 current-starved delay cells similar to the one proposed in [13] to measure the extra delay that may appear between dies. Unlike [13], for our investigation the test structure was only needed on a small number of TSVs; it did not need to be repeated for all TSVs. The ring oscillator was modelled in SPICE with 65 nm technology CMOS. The overall delay associated with the TSVs was dominated by the TSVs' capacitances and the drivers' resistances [19], [20]. For our investigation, the 3D ring oscillators' delay was measured as the delays of the TSVs that connect the layers, the driver circuitry, and the inverters. Routing delays between inverters in the *same* layer were ignored as they are a very small component of the overall delay.

Consider a 3D IC consisting of four face-up dies shown in Figure 1(a). The initial proposed 3D ring oscillator test structure for detecting an extra die measured the signal delay from the bottom die to each die in the 3D stack [12]. For this circuit, three separate ring oscillators were used to measure the delay from the bottom die 1 to die 2, die 3 and the top die in the stack respectively. Now consider a compromised stack with an extra Trojan die between die 3 and die 4 as shown in Figure 1(b). In this case, the presence of an extra Trojan die caused a 93% increase in the delay of the 3D ring-oscillator encompassing all dies in the stack.

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. 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

Authorized licensed use limited to: SOUTHERN METHODIST UNIV. Downloaded on June 04,2021 at 22:11:09 UTC from IEEE Xplore. Restrictions apply.

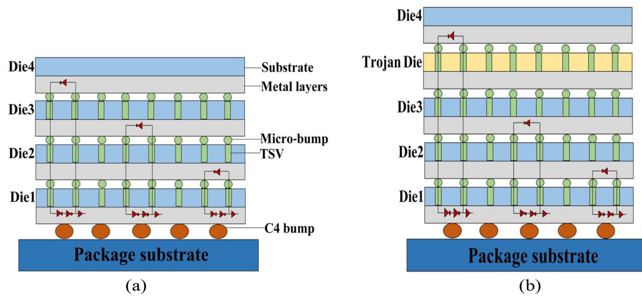


FIGURE 1. Circuit 3D ROs tests. (a) Test structure without a Trojan die. (b) Test structure with a Trojan die between the die 3 and die 4 [12].

dies. Because coordination between die providers is challenging today, this is a critical issue. This coordination would be needed due to the design of the test structure, which consists of a series of ROs starting from the base die (Die1) to each die above, and then back to the bottom die (i.e., 3D RO test from Die1 to Die2, 3D RO test from Die1 to Die3, and 3D RO test from Die1 to Die4, etc.). Thus, this technique would require information such as the number of dies in a stack and the location of each die in the stack. Furthermore, all counters would need to be located on the bottom die for the structure shown in Figure 1. Alternatively, space may 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. Specific TSV locations could be standardized and allocated for the test structure that would be the same on every die in the stack. Unfortunately, other portions of the test structure (such as the RO components) would also need to be repeated on all dies even if they are not ultimately connected when the die that will ultimately serve as the bottom die is unknown. This is wasteful of area resources. An alternative approach that leads to easier standardization will be introduced in the next subsection.

In the previous experiment from [12], we did not consider process variations during circuit simulation. However, significant process variations could make it more difficult to clearly attribute the delay difference to an extra Trojan or natural delay variations. To investigate this, we performed Monte Carlo simulation using SPICE while assuming a Gaussian

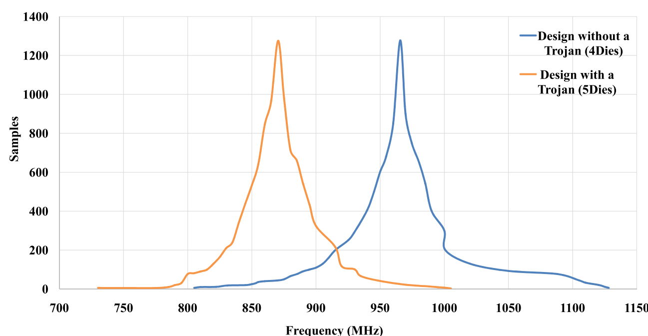


FIGURE 2. Monte Carlo simulation of die stack from Figure 1.

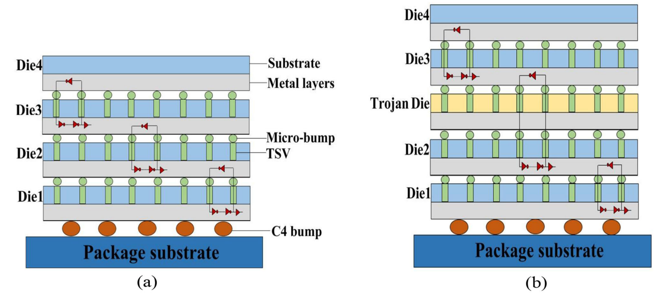


FIGURE 3. Test structure with 3D ROs encompassing two dies. (a) Trojan-free stack. (b) Test structure with a Trojan die [12].

distribution for the variation with 65 nm technology over 10,000 samples to reflect process variations. The Monte Carlo analysis was done by giving a tolerance interval to five parameters — 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). The 3σ value of the distribution for each parameter was set to 10% from the nominal values, and all of the parameters were varied simultaneously.

Figure 2 shows the Monte Carlo simulation results for a 3D ring oscillator in the form of a frequency distribution across 10,000 samples for the four die stack of Figure 1(a) and the one with a Trojan die shown in Figure 1(b). We observe that the process variations in the test components produce significant natural variation in the frequencies of the ring oscillators even when no extra dies are present. Even though the average difference in oscillation frequency is approximately 95 MHz, there is still significant overlap in the distributions. This overlap might cause Trojan dies to be missed or raise many false alarms, depending on what threshold value is chosen to indicate a potential extra die.

2) MODIFYING THE TEST STRUCTURE TO INCREASE THE IMPACT OF THE EXTRA DIE

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 3(a), where each test RO only encompasses two legitimate dies.

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 3(b). The results of Monte Carlo simulation of 10,000 circuit samples with the same (3σ) variation show that the two distributions are now distinct with no significant overlap, as shown in Figure 4.

In addition to avoiding any false alarms or missed Trojans, 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 and ring oscillator components because the order of the stacked dies does not need to be known *a priori*. It is no longer necessary to place all of the RO components on the bottom die. Instead, each

Authorized licensed use limited to: SOUTHERN METHODIST UNIV. Downloaded on June 04,2021 at 22:11:09 UTC from IEEE Xplore. Restrictions apply.

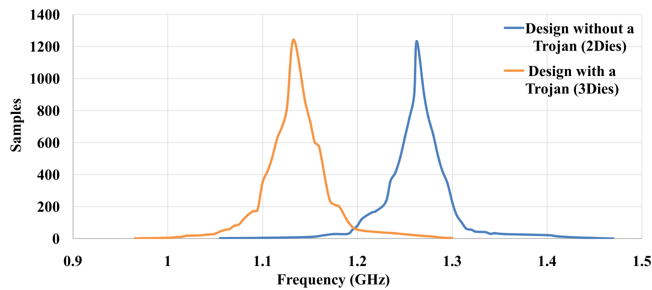


FIGURE 4. Monte Carlo simulation of 10,000 circuit samples of the test structure with 3D ROs encompassing two dies.

die can contain the appropriate components and TSV connections to connect to the dies above and below. Only the top and bottom dies would have unnecessary circuitry added due to the lack of a vertical neighbor. As a result, 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).

The ability to access and extract information from the counters that store data that correspond to the RO delay values 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 test network on each die [21], where the IEEE 1687 network is accessed through the IEEE P1838 test elevator interface. In addition, to prevent defective ROs or TSVs from incorrectly 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.

So far, we have shown that the proposed test structure of 3D ring oscillators encompassing two dies can detect and locate an extra die between stacked dies even in presence of process variation of 10% (3σ) from the nominal values. Next we build on our prior work [12] to consider how a determined attacker might try to conceal the presence of the Trojan die and how we might be able to thwart such concealment.

IV. WHAT MIGHT A DETERMINED ATTACKER DO?

There are several methods that a determined attacker might use to modify the stack to hide the added delay, such as varying the size of the TSVs, modifying dielectric thickness surrounding the TSV, or even duplicating the inverters of the 3D ring oscillator in the Trojan die to avoid detection. In this section, we explore the degree to which different modifications, if done by the attacker, may impact our ability to detect an extra die with delay measurements.

A. REDUCE THE TSV SIZE TO HIDE THE ADDED DELAY

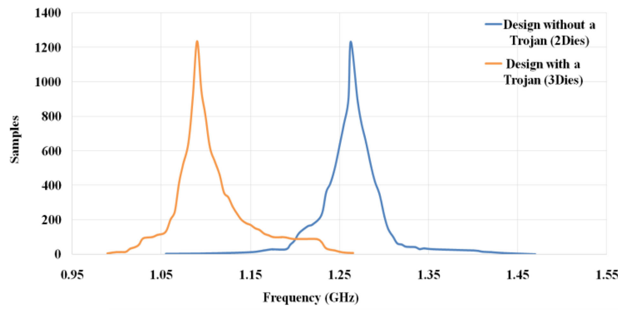
TSV size has a significant impact on the 3D ring oscillator period. In practice, TSV height is equal to the thickness of the die [17], [22], [23], [24], [25], [26], and the TSV footprint is determined by its aspect ratio [27]. Therefore, an attacker can attempt to take advantage of this to hide the added delay and to avoid detection by reducing the size of the TSVs of the Trojan die. For example, the attacker can insert a Trojan die with a small die thickness (which means small TSV height) or can insert one with small footprint TSVs. Thus, the delay added by the Trojan die could be hidden with the presence of process variations. However, this reduction is not necessarily trivial. Decreasing the size of the TSV indicates small wafer thickness that might cause wafer cracking [22]. In addition, reducing the TSV radius would increase the aspect ratio which increases the challenge in deposition isolation layers surrounding the TSV that causes copper diffusion or current leakage [22]. Nonetheless, there is still a possibility that an attacker could attempt this approach, and thus, it is important to evaluate its effectiveness.

TABLE 1. Detecting a Trojan die with small TSVS by using 3D ROs encompassing two dies.

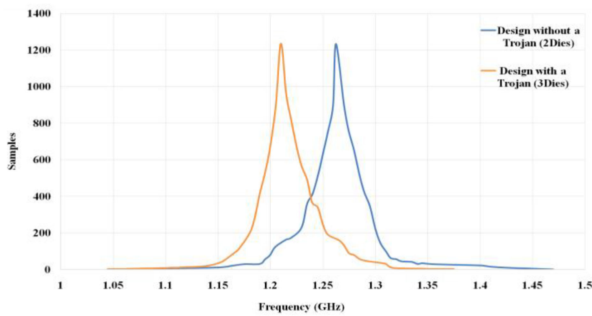
Trojan-die Cases (μm) H=Height D=Diameter	Oscillation Period of 3D ROs Encompassing Two Dies		
	Without a Trojan	With a Trojan	Change (%)
(a) Trojan-free TSVs: H=30, D=2.5 Trojan die TSVs: H=30, D=2	787 ps	917 ps	17%
(b) Trojan-free TSVs: H=30, D=2.5 Trojan die TSVs: H=15, D=1.25	787 ps	837 ps	6%
(c) Trojan-free TSVs: H=50, D=4.17 Trojan die TSVs: H=30, D=2.5	1005 ps	1130ps	12%
(d) Trojan-free TSVs: H=50, D=4.17 Trojan die TSVs: H=20, D=1.7	1005 ps	1070 ps	6%

To examine the effect that different TSV sizes could have on the ring oscillator period and the corresponding ability of an attacker to hide an extra die, we explore the ability of the 3D RO test structure encompassing two dies as shown on Figure 3 to detect a Trojan die. We investigate the effect of four different combinations of TSV dimensions for the Trojan and legitimate dies on the period of oscillation of the RO, as shown in Table 1. In all cases the dielectric thickness is equal to 1 μm. The results shown in Table 1 indicate that the dimensions of the TSVs in the Trojan die can significantly reduce the difference in RO period between a legitimate and Trojan stack. For example, comparing rows (a) and (b) shows that decreasing the size of the TSVs can reduce the increase in RO period from 17% to 6% in the presence of a Trojan. The comparison between rows (c) and (d) are similar and show a reduction from 12% to 6%. Figure 5 shows the RO frequency distributions for the four cases shown in Table 1 in the presence of 10% (3σ) process variations. Clearly, the overlap between the distributions increases significantly when the TSVs in the Trojan dies are smaller (a versus b and c versus d). Thus, if an attacker is able to successfully reduce the TSV sizes in the Trojan die, it more likely that a stack with the Trojan may escape the detection process.

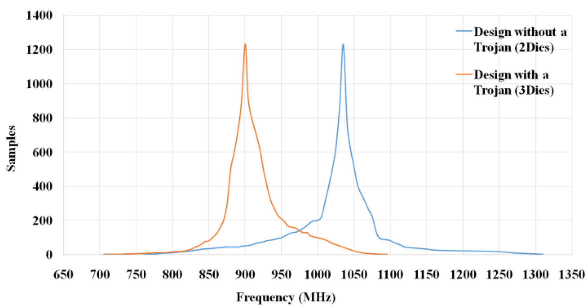
Authorized licensed use limited to: SOUTHERN METHODIST UNIV. Downloaded on June 04,2021 at 22:11:09 UTC from IEEE Xplore. Restrictions apply.



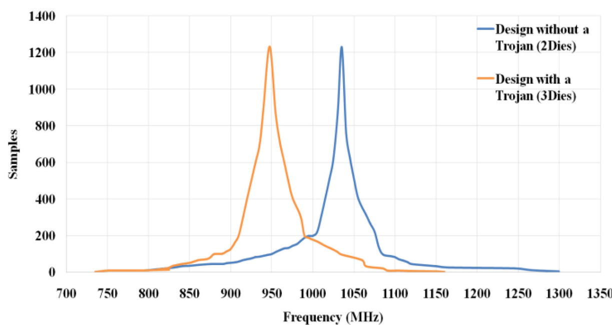
(a) Trojan-free TSVs: H=30, D=2.5 Trojan die TSVs: H=30, D=2



(b) Trojan-free TSVs: H=30, D=2.5 Trojan die TSVs: H=15, D=1.25



(c) Trojan-free TSVs: H=50, D=4.17 Trojan die TSVs: H=30, D=2.5



(d) Trojan-free TSVs: H=50, D=4.17 Trojan die TSVs: H=20, D=1.7

FIGURE 5. Monte Carlo simulation of 10,000 circuit samples of the 3D RO test structure encompassing two dies when an attacker reduces the TSV size in the Trojan die.

TABLE 2. Measuring the TSV capacitance and the 3D RO delay with different dielectric thicknesses.

Different Dielectric Thickness TSV Height=30 μm TSV diameter=2.5 μm	TSV Capacitance	Measurement for Trojan-free 3D RO (Period)
0.1 μm	84.4924 fF	1562 ps
0.2 μm	43.8123 fF	1183 ps
1 μm	11.0629 fF	787 ps

B. MODIFY THE DIELECTRIC THICKNESS

TSVs are electrically isolated from the Si substrate by using an isolation layer (sidewall dielectric). This liner layer determines the TSV capacitance [17], [18] — an increase in the isolation layer thickness reduces the TSV parasitic capacitance [27], [28]. Reducing the TSV capacitance in turn will reduce the overall delay through the TSV. However, increasing the isolation layer thickness decreases the peak substrate noise, and it also results in an area penalty and large interconnect blockages [24]. In this attack model, an attacker might be unconcerned with the added area penalty or decrease in the peak substrate noise and might make modifications to the dielectric thickness to hide the added impact of the Trojan die to the overall delay. To examine the effect that different dielectric thickness could have on the TSV capacitance and delay, we increase the sidewall dielectric thickness of the TSV and measure the TSV capacitance and the 3D RO period. Table 2 shows how increasing the sidewall dielectric thickness would reduce the capacitance of the TSV and the period.

To measure the impact that increasing dielectric thickness could have on the ability of an attacker to hide a Trojan die, we obtain the frequency of a non-Trojan 3D ring oscillator with 0.1 μm TSV dielectric thickness. Then, we insert a Trojan die between die 1 and die 2 with 1 μm dielectric thickness of the TSVs, and we estimate the frequency by using the test structure that encompasses two dies as shown in Figure 3. Our experiments show that Trojan inserted die with a thicker dielectric TSV resulted in an overall period of 1,667 ps. This was only a 7% increase over a Trojan free case as shown on the first row of Table 2 making it difficult to detect the modified TSV based Trojan especially in the presence of process variations. Our Monte Carlo simulation results with the same parameters and setup as described previously is shown in Figure 6. We see a significant overlap in the distributions indicating a possibility of many false alarms or missed Trojan dies if the attacker increases the dielectric thickness of the TSVs in the Trojan die.

C. USE THE TROJAN DIE TO COMPLETE THE RO

Another possible method that a determined attacker could implement to avoid detection is to 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, as shown in Figure 7. Compared to the other two

Authorized licensed use limited to: SOUTHERN METHODIST UNIV. Downloaded on June 04,2021 at 22:11:09 UTC from IEEE Xplore. Restrictions apply.

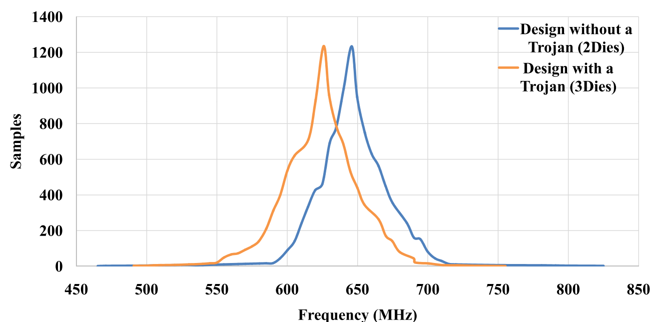


FIGURE 6. Monte Carlo simulation of 10,000 circuit samples of the 3D RO test structure encompassing two dies when an attacker increases the TSV dielectric thickness of the Trojan die.

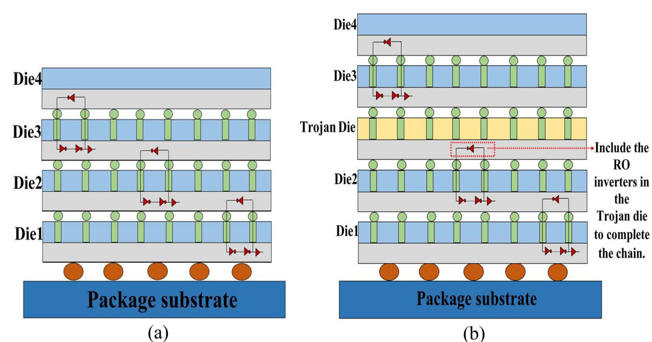


FIGURE 7. Duplicate 3D RO parts. (a) Trojan-free stack. (b) Test structure with a Trojan die.

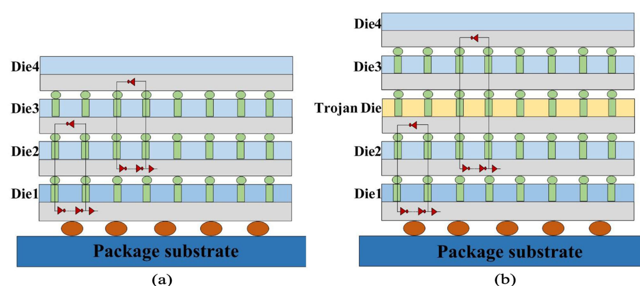


FIGURE 8. Test structure with 3D ROs encompassing three dies. (a) Trojan-free stack. (b) Test structure with a Trojan die.

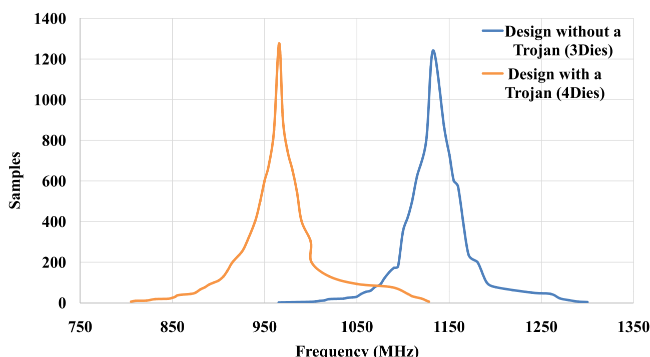


FIGURE 9. Monte Carlo simulation of 10,000 circuit samples of 3DROs encompassing three dies (Trojan-free stack) and 3D ROs encompassing four dies (with a Trojan die).

methods outlined earlier to avoid detection of the Trojan die, it is likely more difficult to duplicate the ring oscillator inverters because it is not easy for the attacker to distinguish which ring oscillators in the chip are used in the test structure. Furthermore, the original 3D dies could contain multiple 3D ring oscillator test structures to either distinguish between the extra delay added by the Trojan die or to detect defective TSVs. In such a scenario, while the duplication of the ROs in the Trojan die is still a possibility, it would make it slightly harder for an attacker to accomplish the full duplication of all ring oscillator paths.

So far, we have seen that the 3D ring oscillator based test structure that encompasses two dies in a stack provides the ability to detect an inserted Trojan die. We have also seen that process variation can lead to some uncertainty in the conclusive detection of a Trojan Die, and a determined attacker could modify the TSV's size or dielectric thickness on the Trojan die to take advantage of process variation based uncertainties to hide the die. In Section V, we propose alternate ring oscillator structures to provide a better detection probability even in presence of process variation and even with the different measures an attacker might take to hide the die.

V. ALTERNATE TEST STRUCTURE WITH 3D RING OSCILLATORS

In Section IV-C, we saw that a determined attacker could potentially duplicate the ring oscillator parts on the Trojan die to mask its existence. Instead of the two die structure shown earlier, an alternate 3D ring oscillator structure that includes three instead of the two dies (for the example stack shown in Figure 7(a)) could be used. If the 3D circuit consists of n dies, we would need $(n\text{-}2)$ 3D ring oscillators that encompass three dies. For example, if the 3D stack consists for a total of four dies, two 3D ring oscillators should be placed for this purpose (e.g., from die 1 to die 3 and from die 2 to die 4) as shown in Figure 8. Our simulations show that there is a 14% increase in the average RO period for the Trojan die inserted stack (shown in Figure 8(b)) over the Trojan free case (Figure 8(a)).

To investigate the effectiveness of this test structure with the presence of process variation, we perform a Monte Carlo simulation with the variation of 10% (3σ) for a 3D ring oscillator without a Trojan (3 dies) and the same 3D ring oscillator with a Trojan die (4 dies). Figure 9 shows that this method is able to detect the Trojan die. However there still exists the possibility of incorrect determination because of the small overlap seen in the distributions.

A. INCORPORATING MULTIPLE TSVS FOR A SINGLE 3D RING OSCILLATOR BETWEEN TWO DIES

To deal with the methods previously described that could be used by an attacker to hide the delay inserted by a Trojan die, we propose another test structure in which a single 3D ring oscillator traverses additional TSVs between two dies. For

Authorized licensed use limited to: SOUTHERN METHODIST UNIV. Downloaded on June 04,2021 at 22:11:09 UTC from IEEE Xplore. Restrictions apply.

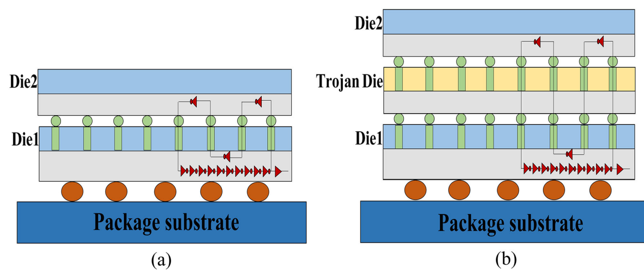


FIGURE 10. Test structure with 3D ROs incorporating multiple TSVs (four TSVs). (a) Trojan-free stack. (b) Stack with a Trojan die.

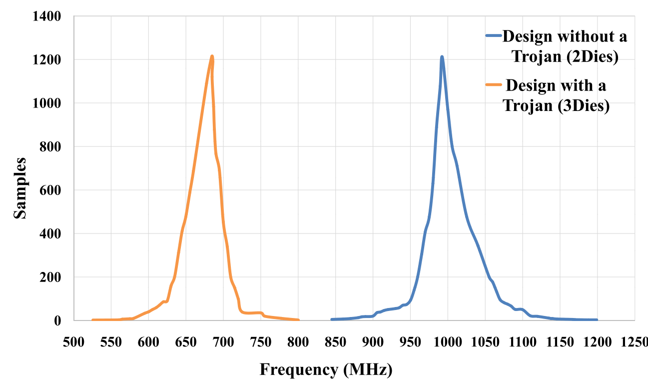


FIGURE 11. Monte Carlo simulation of 10,000 circuit samples of the test structure with 3D RO incorporating four TSVs.

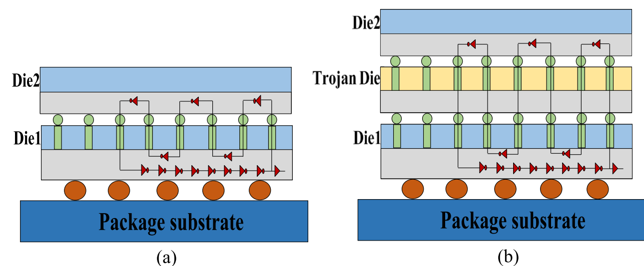


FIGURE 12. Test structure with 3D ROs incorporating multiple TSVs (six TSVs). (a) Trojan-free stack. (b) Stack with a Trojan die.

example, a 3D ring oscillator might go through four TSVs instead of just two TSVs between two dies to further separate the delay distribution for a legitimate and Trojan stack, as shown in Figure 10(a). In a stack without a Trojan, the oscillation period of the RO is equal to 1,000 ps. However, the oscillation period with a Trojan die (Figure 10(b)) stack increases to 1,504 ps. By using this test structure, the presence of the Trojan die causes a 50% increase in delay value between two dies over the value expected when no Trojan die is present in the stack.

To further account for process variations, we perform 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 die 1 and die 2 as shown in Figure 10(b). The result of the Monte Carlo simulation of 10,000 circuit samples with

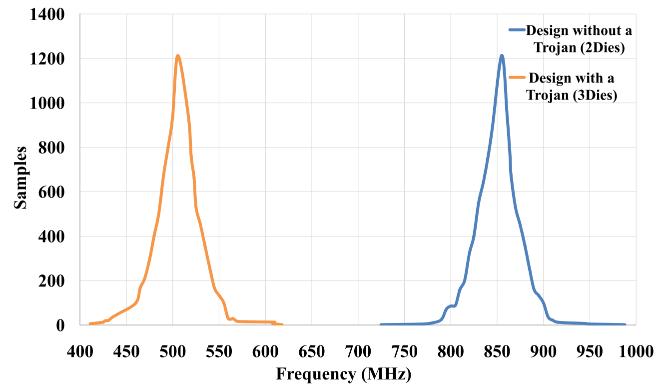


FIGURE 13. Monte Carlo simulation of 10,000 circuit samples of the test structure with 3D RO incorporating six TSVs.

TABLE 3. Comparing the ability of test structure with 3D ROs incorporating multiple TSVs to detect Trojan dies.

Test Structure	Trojan Free Stack (Period)	Stack with Trojan die (Period)	% Change
2 TSVs	787 ps	939 ps	19%
4 TSVs	1000 ps	1504 ps	50%
6 TSVs	1176 ps	1980 ps	68%

the same 10% (3σ) variation shows that the two distributions are now more distinct, as shown in Figure 11.

Furthermore, we can incorporate more TSVs in the test structure, in which a 3D ring oscillator goes through six TSVs instead of just two TSVs between two dies as shown in Figure 12(a). By measuring the delay of the Trojan-free RO and a compromised RO, the oscillation periods are 1,176 and 1,980 ps, respectively. The presence of the Trojan die causes a 68% increase in delay value between two dies over the value expected when no Trojan die is present in the stack. Thus, the extra delay is increased as the number of the included TSVs in the test structure is increased. The Monte Carlo simulation result shown in Figure 13 for a 3D ring oscillator without a Trojan (2 dies) and the same 3D ring oscillator with a Trojan die between die 1 and die 2 as shown in Figure 12(b) shows that the two distributions are even more separated. This structure is beneficial as it allows us to determine with high degree of certainty when a Trojan die is inserted.

Table 3 summarizes results for the proposed test structures that incorporate two, four, and six TSVs between two dies, and presents the RO period and the percentage change introduced by the Trojan die. The table confirms that as more TSVs are used in the 3D RO structure, the ability to identify insertion of a Trojan die improves substantially. Intuitively, this occurs because adding TSVs to the test structure in a good stack increases the number of times the RO signal must pass between the two dies. If a Trojan die is added to the stack, then extra delay is added for every traversal and the total delay added by the Trojan die is increased.

Authorized licensed use limited to: SOUTHERN METHODIST UNIV. Downloaded on June 04,2021 at 22:11:09 UTC from IEEE Xplore. Restrictions apply.

TABLE 4. Detecting a Trojan DIE with small TSVS by using the test structures that incorporate multiple TSVS (4 or 6 TSVs) between two dies.

Trojan-die Cases (μm)	Oscillation Period of 3D ROs Incorporating Four TSVs			Oscillation Period of 3D ROs Incorporating Six TSVs		
	With Trojan	Without Trojan	Change	With Trojan	Without Trojan	Change
(a) Trojan-free TSVs: H=30, D=2.5 Trojan die TSVs: H=30, D=2	1000 ps	1439 ps	44%	1176 ps	1869 ps	59%
(b) Trojan-free TSVs: H=30, D=2.5 Trojan die TSVs: H=15, D=1.25	1000 ps	1220 ps	22%	1176 ps	1538 ps	31%
(c) Trojan-free TSVs: H=50, D=4.17 Trojan die TSVs: H=30, D=2.5	1429 ps	2062 ps	44%	1802 ps	2857 ps	59%
(d) Trojan-free TSVs: H=50, D=4.17 Trojan die TSVs: H=20, D=1.7	1429 ps	1852 ps	30%	1802 ps	2539 ps	41%

B. HOW MIGHT AN ATTACKER RESPOND TO THIS NEW STRUCTURE?

While these new test structures provide a higher degree of detection of an inserted Trojan die, a determined attacker might employ the same approaches described in Section IV to conceal the presence of the Trojan die. We now test the new structure against the attacker's circumvention approaches.

1) REDUCE THE TSV SIZE TO HIDE THE ADDED DELAY

In Section IV we described how a determined attacker might hide the delay associated with the Trojan die by modifying the height and diameter of the TSVs. To examine the ability of the test structures incorporating four and six TSVs between two dies to detect the Trojan die even when an attacker attempts to reduce the TSVs sizes of the Trojan die, we investigate the oscillation frequencies obtained for these test structures. We perform experiments with the same assumptions that were used in Section IV regarding the TSVs' sizes that are placed in the Trojan die and good dies to validate the efficiency of the proposed techniques for detection.

The increased delay for all cases are shown in Table 4. We see that even when the attacker tries to reduce the extra delay caused by the Trojan die by decreasing the TSVs' size, these test structures integrating multiple TSVs are more effective than the other test structures for detecting the Trojan die. Moreover, the Monte Carlo simulations are performed by using the same variation for all cases as shown in Figure 14, which shows that these techniques are more promising. This is especially true for the method that includes six TSVs in the test structure.

2) MODIFY THE DIELECTRIC THICKNESS

To measure the impact of an attacker modifying the dielectric thickness, we examine the frequency of a non-Trojan 3D ring oscillator with 0.1 μm TSV dielectric thickness. Then, we insert a Trojan die between die 1 and die 2 while increasing the TSV dielectric thickness of the Trojan die to 1 μm. On average we see the RO period increases from 2,778 ps to 3,846 ps (a 38% increase) for the test structure incorporating 4 TSVs. Similarly, the RO period increases by 49% (from 3,846 ps to 5,714 ps) when 6 TSVs are involved. A Monte Carlo simulation to model the process variation is performed for these test structures that incorporate 4 TSVs and 6 TSVs. The results in Figure 15 show that these new structures are more promising for detection of a Trojan die even when the attacker attempts to modify the dielectric thickness.

3) DUPLICATE 3D RING OSCILLATOR PARTS

As discussed in Section IV, 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. This will require the attacker to identify the location of TSVs that are used for the test, and add appropriate RO inverters in the Trojan die to complete the test structure. We therefore examine the test structures that incorporate multiple TSVs when these structures include three dies instead of two dies. Table 5 shows the oscillation period that arises when a 3D RO encompasses three dies (in a Trojan-free stack) versus a 3D RO that encompasses four dies (with a Trojan die); unsurprisingly, the oscillation period increases as the number of included TSVs increases.

To investigate the effectiveness of these test structures with the presence of process variation, we also performed a Monte Carlo simulation for a 3D ring oscillator without a Trojan and the same 3D ring oscillator with a Trojan die. As shown in Figure 16, the results of the Monte Carlo simulation show that including these test structures could effectively detect the Trojan die even if the attacker includes the ring oscillator's inverters in the malicious die.

VI. DISCUSSION AND CONCLUSIONS

In this article, we have introduced approaches to detect an inserted Trojan 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

Authorized licensed use limited to: SOUTHERN METHODIST UNIV. Downloaded on June 04,2021 at 22:11:09 UTC from IEEE Xplore. Restrictions apply.

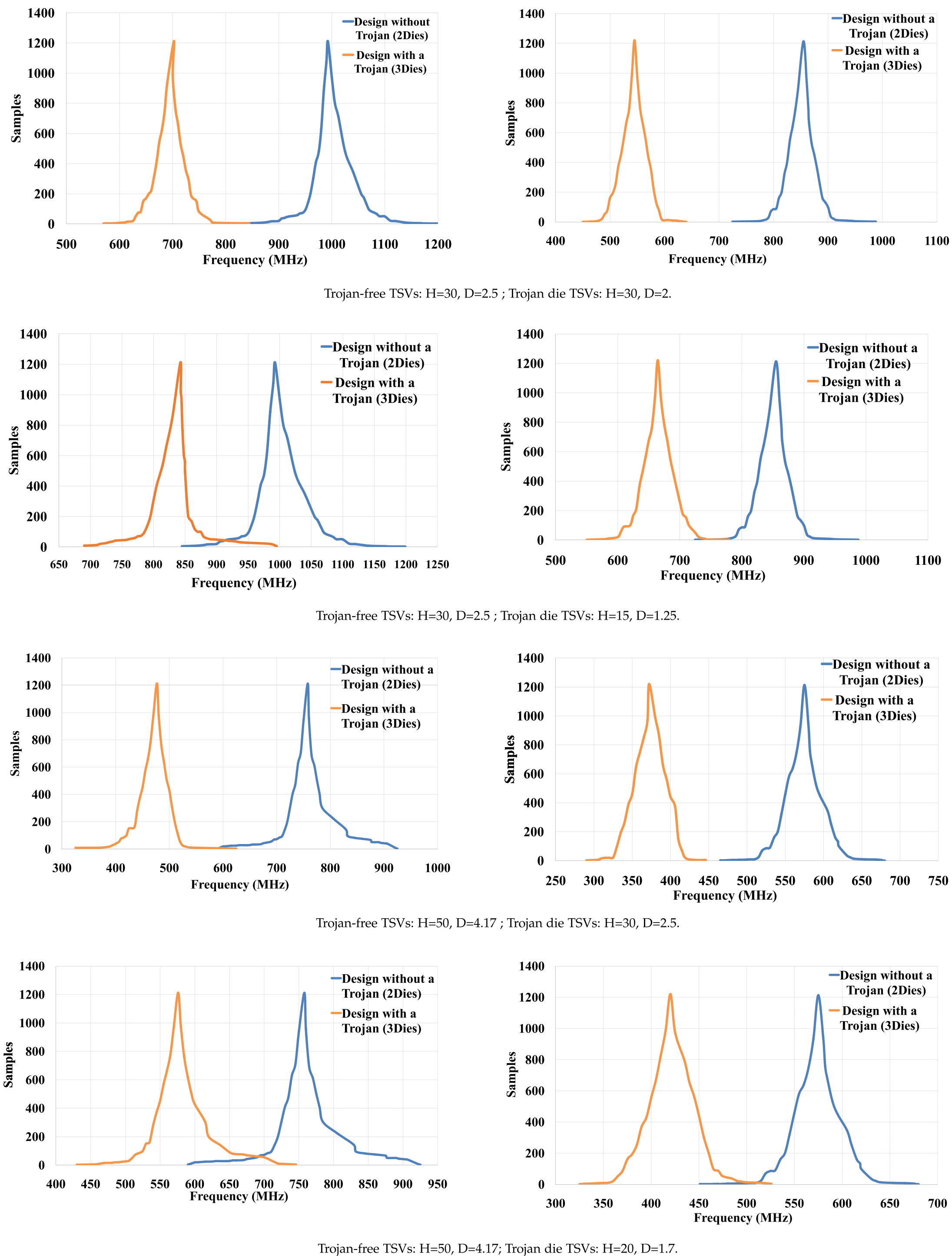
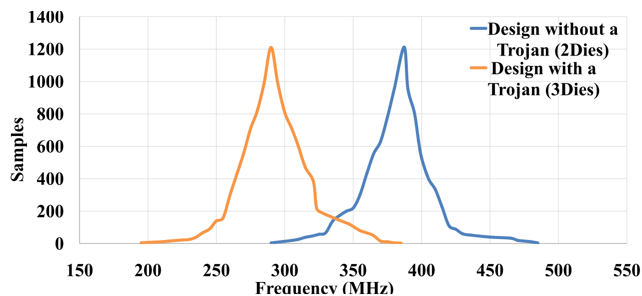


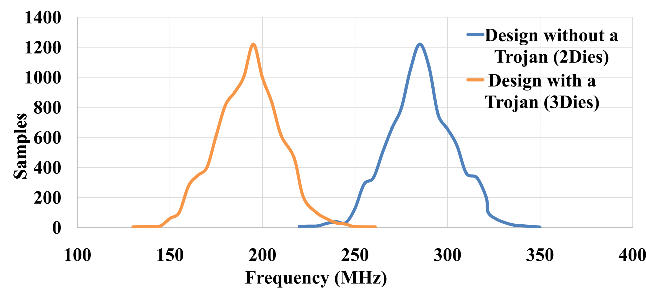
FIGURE 14. Monte Carlo simulation of 10,000 circuit samples of the test structures that incorporate (a)four TSVs and (b)six TSVs when the attacker reduces the TSVs size to hide the Trojan die.

testing. In this work, we have experimented with a number of 3D ring oscillator based test structures. With these structures, we can detect and locate an extra die between stacked die with the variation of 10% (3σ) from the nominal values. We have proposed a 3D RO based test structure that is based on the bottom of the stack and that incorporates multiple upper dies. This test structure can be used to detect the extra delay and identify and locate the presence of a Trojan die under ideal conditions. However, when process variation is considered, the increased delay in a stack with a Trojan die can be

Authorized licensed use limited to: SOUTHERN METHODIST UNIV. Downloaded on June 04,2021 at 22:11:09 UTC from IEEE Xplore. Restrictions apply.

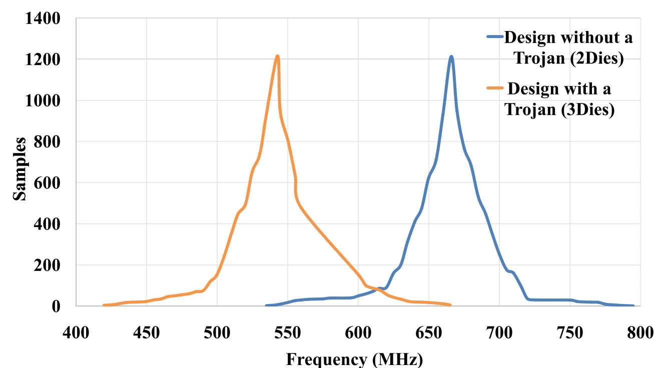


(a) Incorporating 4 TSVs in the test.

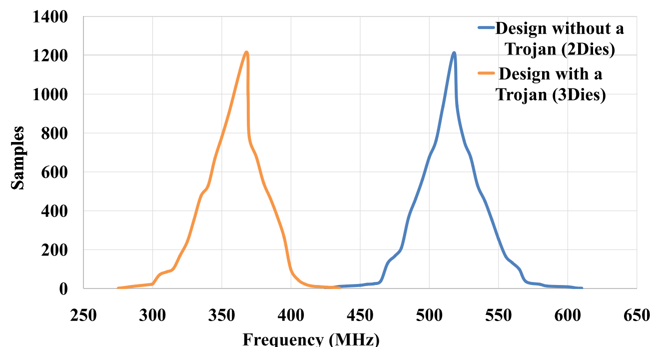


(b) Incorporating 6 TSVs in the test.

FIGURE 15. Monte Carlo simulation of 10,000 circuit samples of the test structures that incorporate multiple TSVs when the attacker increases the dielectric thickness of the Trojan die's TSVs.



(a) Incorporating 4 TSVs in the test.



(b) Incorporating 6 TSVs in the test.

FIGURE 16. Monte Carlo simulation of 10,000 circuit samples of Test Structure that Incorporates Multiple TSVs with 3D ROs encompassing three dies (Trojan-free stack) and 3D ROs encompassing four dies (with a Trojan die).

harder to detect reliably with this structure. Thus, an alternative ring oscillator-based test structure that distributes the test structures so that each test structure focuses on the delay between two legitimate dies only is proposed to better handle process variations. With this test structure, we can detect and locate an extra die between stacked dies with a process variation of 10% (3σ) from the nominal values. Moreover, the test structures incorporating multiple TSVs between two dies are more promising to detect the Trojan die even when the attacker attempts to modify the TSV's characteristics, such as height, diameter, and dielectric thickness.

We have also characterized the RO based test structures for Trojan detection when the attacker includes the ring oscillator's inverters in the Trojan die itself and completes the chain in the Trojan die to avoid detection. An additional test structure encompassing three dies was shown to be capable of defeating such an attack.

TABLE 5. Detecting a Trojan die by using the test structure that incorporates multiple TSVS with the 3D RO encompassing three dies (Trojan-free stack) and 3D RO encompassing four dies (with a Trojan die).

Test Structure	Measurement for Trojan-free stack	Measurement for a stack with a Trojan Die	Result
	Delay(Dref)	Delay(D)	Change(%)
4 TSVs	1504 ps	2020 ps	34%
6 TSVs	1980 ps	2778 ps	40%

There is always an inherent tradeoff between security and overhead/cost. The choice of the best test structure is dependent upon how much security is needed and how much cost is acceptable.

One challenge in using delay measurements to detect Trojans is that defects may also cause an additional delay which could be erroneously interpreted as indicating the presence of a Trojan. By adding a second redundant set of the test structures proposed in this work and comparing the delay between the two sets, we can better differentiate between delays due to defects and the presence of a Trojan die (which would affect both sets).

The proposed test structures require extra effort from the industry to coordinate the necessary structures on each die among different die providers. Ideally, the industry could develop a security standard that leaves space for specific locations for the TSVs and provides the RO components necessary to make the needed test structures. This is especially appropriate if the test structure in Figure 3 (or another test structure that only encompassed two dies) is used.

Our future work will further investigate the possibility that a Trojan die is placed on the top or bottom of a stack instead of between layers. Furthermore, we can investigate how other sources of variations (e.g., thermo-mechanical stress, carrier mobility, etc.) might affect the ability of our test structure to

Authorized licensed use limited to: SOUTHERN METHODIST UNIV. Downloaded on June 04,2021 at 22:11:09 UTC from IEEE Xplore. Restrictions apply.

detect the presence of a Trojan die. Finally, we can investigate the impact of various Trojan die insertion approaches on the long-term reliability of a stack and TSVs, regardless of the intended behavior of the Trojan die.

REFERENCES

[1] 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, Second Quarter 2016.

[2] J. Ellis, "A call to action on 3D IC security." Accessed: Nov. 1, 2016, 2012. [Online]. Available: http://chipsecurity.org/2012/03/a-call-to-action/

[3] E. Worthman, "Designing for security," 2015. [Online]. Available: http://semiengineering.com/designing-for-security-2/

[4] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor, "Hardware trojans: Lessons learned after one decade of research," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 22, no. 1, pp. 6:1–6:23, May 2016. [Online]. Available: http://doi.acm.org/10.1145/2906147

[5] J. Ellis, "Are stacked die creating new security risks?" Accessed: Jun. 12, 2017, 2015. [Online]. Available: https://www.rambus.com/blogs/are-stacked-die-creating-new-security-risks-2/

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

[7] C. Wang *et al.*, "BIST methodology architecture and circuits for pre-bond TSV testing in 3D stacking IC systems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 1, pp. 139–148, Jan. 2015.

[8] 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," in *Proc. 20th Asia South Pacific Des. Autom. Conf.*, 2015, pp. 520–525.

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

[10] W. H. Hsu, M. A. Kochte, and K. J. Lee, "3D-IC test architecture for TSVs with different impact ranges of crosstalk faults," in *Proc. Int. Symp. VLSI Des. Autom. Test*, 2016, pp. 1–4.

[11] 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," in *Proc. IEEE 11th Int. New Circuits Syst. Conf.*, 2013, pp. 1–4.

[12] S. Alhelaly, J. Dworak, T. Manikas, P. Gui, K. Nepal, and A. L. Crouch, "Detecting a trojan die in 3D stacked integrated circuits," in *Proc. IEEE North Atlantic Test Workshop*, 2017, pp. 1–6.

[13] 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.

[14] R. Verplancke, T. Sterken, D. Cuypers, and J. Vanfleteren, "Thinned dies in a stretchable package," in *Proc. 4th Electron. Syst.-Integr. Technol. Conf.*, 2012, pp. 1–5.

[15] M. Kada and L. Smith, "Advancements in stacked chip scale packaging (S-CSP), provides system-in-a-package functionality for wireless and handheld applications," *J. Surface Mount Technol.*, vol. 13, no. 2, pp. 11–15, 2000.

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

[17] 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, 2010.

[18] ITRS, "International technology roadmap for semiconductors (Interconnect)," 2015. [Online]. Available: http://www.itrs2.net/

[19] 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.

[20] M. Ahmed and M. Chrzanowska-Jeske, "Delay and power optimization with TSV-aware 3D floorplanning," in *Proc. 15th Int. Symp. Qual. Electron. Des.*, 2014, pp. 189–196.

[21] *IEEE Standard for Access and Control of Instrumentation Embedded Within a Semiconductor Device*, IEEE Std 1687–2014, pp. 1–283, 2014.

[22] Q. Chen, C. Huang, and Z. Wang, "Development of ultra-low capacitance through-silicon-vias (TSVs) with air-gap liner," in *Proc. IEEE 63rd Electron. Compon. Technol. Conf.*, 2013, pp. 1433–1438.

[23] N. H. Khan, S. M. Alam, and S. Hassoun, "Power delivery design for 3-D ICs using different through-silicon via (TSV) technologies," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 19, no. 4, pp. 647–658, Apr. 2011.

[24] N. Khan and S. Hassoun, *Designing TSVs for 3D Integrated Circuits*. Hoboken, NJ, USA: Wiley, 2013.

[25] C. Xu, H. Li, R. Suaya, and K. Banerjee, "Compact AC modeling and performance analysis of through-silicon vias in 3-D ICs," *IEEE Trans. Electron Devices*, vol. 57, no. 12, pp. 3405–3417, Dec. 2010.

[26] K. Kondo, M. Kada, and K. Takahashi, *Three-Dimensional Integration of Semiconductors: Processing, Materials, and Applications*. Berlin, Germany: Springer, 2015.

[27] S. M. Alam, R. E. Jones, S. Rauf, and R. Chatterjee, "Inter-strata connection characteristics and signal transmission in three-dimensional (3D) integration technology," in *Proc. 8th Int. Symp. Qual. Electron. Des.*, 2007, pp. 580–585.

[28] X. Wu *et al.*, "Electrical characterization for intertier connections and timing analysis for 3-D ICs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 20, no. 1, pp. 186–191, Jan. 2012.

SOHA ALHELALY received the BS degree in computer science from Um AL-Qura University, Makkah, Saudi Arabia, in 2007, the MS degree from St. Marys University, San Antonio, Texas, in 2011, and the PhD degree in computer science and engineering from Southern Methodist University, Dallas, Texas, in 2017. She is currently an assistance professor of computer science with Saudi Electronic University in Jeddah, KSA. Her current research interests include security and trust in 3D integrated circuits, VLSI design algorithms, and hardware security.

JENNIFER DWORAK (Member, IEEE) received the BS, MS, and PhD degrees in electrical engineering from Texas A&M University, College Station, Texas, in 1998, 2000, and 2004, respectively. She is currently an associate professor of Electrical and Computer Engineering at Southern Methodist University in Dallas, Texas. Her current research interests include manufacturing and in-field testing, reliable systems, and hardware security.

KUNDAN NEPAL (Senior Member, IEEE) received the BS degree in engineering from Trinity College, Hartford, Connecticut, the MSEE degree from the University of Southern California, Los Angeles, California, and the PhD degree in electrical and computer engineering from Brown University, Providence, Rhode Island, in 2002, 2003, and 2007, respectively. He is currently an associate professor of Electrical and Computer Engineering at the University of St. Thomas, Saint Paul, Minnesota. His research interests include defect/fault tolerant circuits and systems, digital VLSI system design, and reconfigurable computing.

THEODORE MANIKAS (Senior Member, IEEE) received the BS degree in electrical engineering from Michigan State University, East Lansing, Michigan, the MS degree in electrical engineering from Washington University, St. Louis, Missouri, and the PhD degree in electrical engineering from the University of Pittsburgh, Pittsburgh, Pennsylvania. He has been with Southern Methodist University since 2009 and is a clinical professor with the Department of Computer Science. His current research interests include system security and testing. He is a licensed professional engineer in Texas and Oklahoma.

Authorized licensed use limited to: SOUTHERN METHODIST UNIV. Downloaded on June 04,2021 at 22:11:09 UTC from IEEE Xplore. Restrictions apply.

PING GUI (Senior Member, IEEE) received the PhD degree from the University of Delaware, Newark, Delaware. She is currently a professor with the Department of Electrical and Computer Engineering, Southern Methodist University, Dallas, Texas. Her current research interests include analog, mixed signal, and RF/millimeter wave IC for a variety of applications, including high-speed wireline and wireless transceiver design, analog-to-digital converter/digital-to-analog converter design, and low-power and low-noise circuits for biomedical applications. She was a recipient of the CERN Scientific Associate Award from 2008 to 2010, the IEEE Dallas Section Outstanding Service Award in 2011, and the Gerald J. Ford Research Fellowship at SMU in 2015.

ALFRED L. CROUCH (Senior Member, IEEE) received the MSEE degree from the University of Kentucky, Lexington, Kentucky. He is the director of hardware engineering with Amida Technology Solutions. Amida is headquartered in Washington DC, but he is located in the Austin, Texas, office and works closely with resources in the Dallas area. His role with Amida is to direct research and development on hardware cybersecurity investigation and remediation products.

Authorized licensed use limited to: SOUTHERN METHODIST UNIV. Downloaded on June 04,2021 at 22:11:09 UTC from IEEE Xplore. Restrictions apply.