2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)

Modeling Hardware Trojans in 3D ICs

Zhiming Zhang
Dept. of Electrical and Computer Engineering
University of New Hampshire
Durham, NH 03824, USA
zz1017@wildcats.unh.edu

Qiaoyan Yu
Dept. of Electrical and Computer Engineering
University of New Hampshire
Durham, NH 03824, USA
qiaoyan.yu@unh.edu

***Abstract*—Three-dimensional (3D) integration facilitates to integrate increasing number of transistors into a single package. Despite of improved performance and power efficiency, the integration of multiple dies into the same package potentially leads to new security threats, such as 3D hardware Trojans. In this work, we first provide a thorough survey of reported hardware Trojans in 3D integrated circuits and systems, and then propose comprehensive 3D hardware Trojan models. A case study is performed to verify the implementation feasibility of thermal-triggered 3D Trojan. The activation speed of the 3D Trojan is compared to its 2D counterpart to confirm that 3D IC provides a better environment to hide thermal Trojans.**

***Index Terms*—3D IC, hardware Trojan, side-channel analysis attack, interconnect, through-silicon via (TSV)**

I. Introduction

Three-dimensional (3D) integration is an emerging technology to ensure the growth in transistor density and performance of future integrated circuits (ICs) [1], [2]. It has been demonstrated that 3D techniques can be leveraged to reduce package size and power consumption while significantly improving bandwidth. Unfortunately, 3D techniques also bring in unique and unexplored security threats to 3D ICs [3]. It is more challenging to address the security threats in 3D ICs than in 2D planar chips.

A larger number of transistors integrated into the single package makes the exhaustive functional testing more sophisticated and time consuming. Limited probing capacity does not allow us to simultaneously access all die-to-die vertical communication channels for thorough functional testing. Although each die and Through Silicon Via (TSV) can be examined during the pre-bond and mid-bond stages, the testing probe may damage some TSVs and thus harm downstream integration [4]. Due to these challenges on traditional testing, malicious component detection via functional testing on 3D ICs is not optimistic [5].

Larger variation on temperature, process, and voltage in 3D ICs may lead to a higher false positive rate if we adopt side-channel signals based hardware Trojan detection methods for 2D circuits. The work [6] provides a temperature distribution comparison among 2D, 2-tier 3D and 4-tier 3D Chip-Multiprocessors (CMPs). That work indicates that the variation on temperature increases with the increasing number of 3D tiers. The standard derivation on temperature for the 4-tier 3D chip is approximately 40 times higher than that for the 1-tier 2D chip. Using an analytical system-level variability model, the work [7] predicts that the performance degradation due to the process variation in a 3D MPSoC is larger than that in the 2D counterpart. The work [7] also predicts that the performance degradation will get even worse when the number of 3D tiers increases, as the process variation in 2D, 2-tier 3D and 4-tier 3D will degrade perform by 8%, 14% and 17%, respectively.

As discussed above, more thorough testing approaches and harmless facility are needed to perform hardware Trojan detection in 3D ICs. To assure the integrity and security of 3D chips, it is imperative to improve our knowledge on potential hardware Trojans in the context of 3D integration. However, the existing work considering 3D-Trojan threats mostly focuses on the Trojan insertion in malicious foundries. Limited work addresses the exact Trojan models which could be implemented in 3D ICs. High-level modeling for 3D Trojans and quantitatively assessment on side-channel signals will benefit the hardware security community to propose effective countermeasures against 3D hardware Trojan insertion. More specifically, our main contributions are as follows.

1) This is the first work that does a thorough survey on hardware Trojans in 3D ICs. Threat models and Trojan models reported in the existing literature are compared in details.
2) Four high-level 3D hardware Trojan models are proposed in this work. Practical examples for each Trojan model is provided, as well.
3) Thermal-induced 3D hardware Trojan is emulated in a platform composed of FPGA, microcontroller, heat generator and heat sink to assess the Trojan trigger/detection speed in a passcode based authentication application.

The rest of this paper is organized as follows: Section 2 briefly introduces the preliminary knowledge on hardware Trojan in 2D ICs. Section 3 summarizes the threat model and hardware Trojan model for 3D Trojans in existing literature. Section 4 proposes comprehensive abstract model of cross-tier 3D Trojan and practical Trojan implementation. Section 5 provides simulation and emulation results for the 3D Trojan implementations. This paper is concluded in Section 6.

II. Preliminaries to Hardware Trojans

Hardware Trojans are malicious modification made on hardware to fulfill attackers' intentions such as sabotaging the original function carried by the target hardware, causing hardware

978-1-7281-3391-1/19/$31.00 ©2019 IEEE
DOI 10.1109/ISVLSI.2019.00093

performance degradation, and leaking confidential information embedded in the hardware. Hardware Trojan insertion could occur in several stages of the IC supply chain, including functional design stage [8], netlist synthesis stage [9], and fabrication stage [10], [11]. The survey paper [12] provides a comprehensive classification of hardware Trojans in terms of Trojan insertion stages, trigger conditions, and payload impact.

A. Trojan Triggering Mechanisms

Depending on how often the hardware Trojan is triggered, the work [13] presents three types of Trojan, always-on, combinational condition and sequential condition. The commonly observed combinational and sequential hardware Trojans [13] typically rely on a group of internal signals to form the rarely triggered condition. While the combinational Trojan enables the payload circuit as soon as the trigger condition is satisfied, the sequential Trojan waits for multiple arrivals of the same trigger condition. An example of always-on Trojan is realized with a ring oscillator, which is composed of eight inverters and causes extra power consumption but not harming the system function. Another example is parametric Trojan, which slightly alters the geometry defined by the sign-off GDSII, doping concentration, dopant polarity, or doping area [14], [15]. As a result, the new voltage transfer characteristic of a CMOS transistor will lead that transistor to have a shifted switching threshold.

B. Trojan Payload Mechanisms

After the arrival of Trojan trigger condition, the operation defined in Trojan payload will be executed. Trojan payload is used to implement attackers' intention, such as modifying the logic value of the original function, or executing malicious operations in hardware. Among different payload designs, covert channel is one of the most challenging payloads for detection. A covert channel generated with the assistance from hardware Trojans could help adversary to extract confidential information, such as the encryption key, without disturbing normal operations of the victim system. A hardware Trojan introduced in [16] monitors the subkey access in the process of encryption and copies the subkeys to an internal memory. After being XORed with the original signal, the encoded subkeys are transmitted via the universal asynchronous receiver transmitter (UART) line. By probing the UART channel, attackers can retrieve the original encryption key. Some hardware Trojans also leverage the internal memory unit to build the covert data channel [17], [18].

III. Our Survey on Existing Hardware Trojans in 3D ICs

A. 3D-Trojan Insertion Scenarios

The increased number of transistors and the vertical dimension integration in 3D ICs potentially leave adversary more exploration space to implement hardware Trojans. As a general trend, more and more chip designs will be outsourced for fabrication. Not all single die fabrication foundries and vertical interconnect (e.g. TSV) manufacturers are trusted.

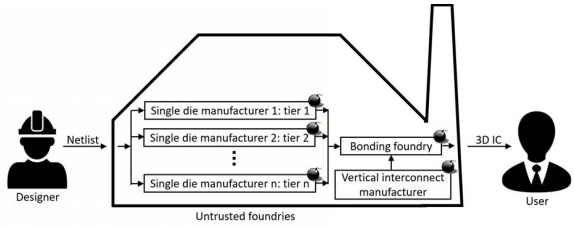

Fig. 1. 3D hardware Trojan insertion in untrusted foundries.

The die-to-die bonding may be performed in an untrusted foundry, too. Figure 1 shows a simplified process of 3D IC manufacturing. We highlight the possible attack surfaces for Trojan insertion. Trojans can be implemented during the single die manufacturing foundries, independently or cooperatively. Since the bonding foundries have access to all the single dies, they have a good chance to implement a Trojan involving multiple dies.

Based on the existing literature, we categorize the 3D Trojans in Table I. We highlight the threat model with special emphasis on threat source and attack target. In addition to Trojan trigger and payload mechanisms, we also point out Trojan locations in the 3D ICs. From the table, we can see that the nature of 3D IC structure creates new opportunities for hardware Trojan design, such as thermal-based Trojans and cross-tier Trojans.

In the next three subsections, we discuss the existing literature listed in Table I according to their special trigger mechanisms and Trojan locations.

B. Thermal Trojans

Thermal issue due to poor heat dissipation in a 3D stack can be exploited to develop Trojan triggering mechanisms. The heat generated and accumulated in the chip will change the electrical parameters of transistors and the switching speed of logic gates. Thus, the system may have new (and unspecified) transition states. The unexpected transition glitches can be exploited as Trojan triggers. This type of hardware Trojans does not need explicit trigger circuits. As indicated in [19], [20], thermal-triggered Trojans can be inserted by any malicious foundries with the access to the layout of design. Those Trojans likely locate near the middle tier, where the heat is harder to dissipate than in other tiers [20]. The work [3] demonstrates that the thermal triggered Trojan may also be hidden in interposer to cause short circuit or these thermal Trojans can be utilized to speedup circuit component aging and consequently lead to Deny-of-Service (DoS).

C. Cross-Tier Trojans

The multiple-die structure of 3D ICs allows attackers to spread the Trojan circuit to multiple tiers. Either the trigger circuit and payload circuit are separated into different tiers, or the trigger circuit being split and located in multiple tiers jointly activates the payload [21]. The Trojans inserted in these ways may bypass the functional testings on individual dies, because those Trojans are not activated by just running tests on individual tiers. The Trojans could be inserted by

TABLE I
EXISTING WORK ON HARDWARE TROJAN IN 3D ICS

Existing Work	Threat Model		Trojan Model		
	Threat source	Attacker access	Trigger	Payload	Location
[19]	Untrusted die foundries	GDSII files	Thermal effect caused transition glitches	No special requirement	Any tiers in 3D
[20]	Untrusted die foundries	GDSII files	Thermal effect caused transition glitches	No special requirement	Middle tier in 3D
[3]	Untrusted interconnect foundries Untrusted single die manufacturers	GDSII files	Thermal effect Aging effect	Voids leading to DoS Partially filled TSVs	Interposer TSV
[21]	Untrusted interconnect foundries Untrusted single die manufacturers Untrusted unified foundries	GDSII files	Remote circuit Distributed circuits	Impacts on target's power Impacts on target's delay	TSV Multiple tiers
[22]	Untrusted single die manufacturers	Least critical die	Low-activity nets	Leak key from encryption unit	Trojan in different tiers with encryption unit
[23]	Untrusted assemblers	No legitimate dies	No special requirement	Interrupt normal function Leak information	Extra Trojan die in 3D stack
[24]	Final bounding foundries	Entire layers	Internal nets	No special requirement	Any tiers in 3D
[25]	Untrusted single die manufacturers	GDSII files	No special requirement	No special requirement	Any tiers in 3D

untrusted die manufacturing foundries, interconnect foundries and unified foundries. The work [22] also introduces a Trojan, which takes advantage of this particular structure of 3D ICs to steal encryption keys. The Trojan and the target encryption unit are located in different tiers and the Trojan is triggered with low-activity nets. Even the untrusted foundry with partial knowledge of the chip can launch this kind Trojan attack.

D. Trojans Exploiting Other 3D Features

The work [23] envisions a new hardware Trojan in stacked 3D ICs: a malicious die is placed between other tiers in the 3D stack. That malicious die carrying Trojan circuits may interrupt normal operations in other 3D tiers or store secret information passing through the Trojan tier. Due to the prominent process variation in 3D chips, the extra delay induced by the 3D hardware Trojan is difficult to be differentiated from process variation. This type of Trojans can be inserted by untrusted assemblers even without the access to legitimate dies. The work [24] introduces the scenarios that attackers are in the foundry who bonds all the outsourced dies. In [25], the adversaries are untrusted die manufacturing foundries with the access to GDSII files. These two works [24], [25] do not have thorough discussions on exact Trojan models.

IV. PROPOSED COMPREHENSIVE 3D-TROJAN MODELS

The major difference between 2D and 3D hardware Trojans is whether or not the Trojan trigger and payload circuits is located in the same tier where the target circuit resides. In 2D chips, the Trojan circuit co-exists with the victim in the same tier. One could perform testing or side-channel analysis to detect the presence of 2D Trojans. In contrast, conventional testing on 3D chips is done in a separated fashion. The die for each tier is tested individually before 3D integration. Once the good dies are stacked vertically, very limited testing will be performed to detect the defects between die-to-die connections, rather than extensively examining the correctness of the 3D system behaviors.

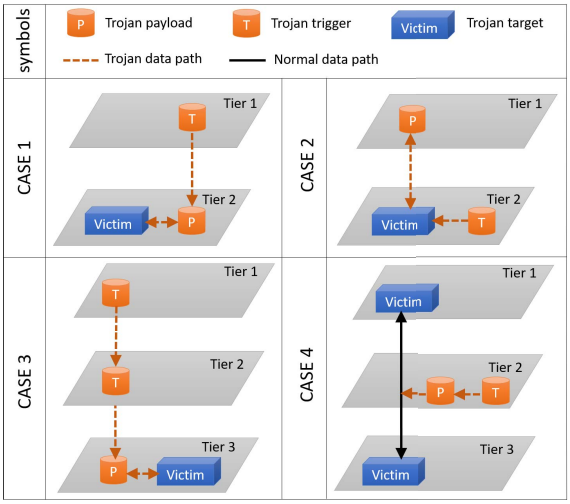

Fig. 2. Proposed four categories of 3D Trojans models.

Based on our survey in Section III, we propose four 3D Trojan models shown in Fig. 2. To the best of our knowledge, this is the first work that introduces comprehensive high-level 3D-Trojan models. In cases 1, 2, and 3, the Trojan trigger circuit and payload circuit are located in different 3D tiers. The case 4 describes the always-on Trojan, in which the payload circuit is on the tier that does not carry the victim circuit. The following subsections will discuss the four Trojan cases.

A. Cross-Tier Trojan Trigger

In case 1, the trigger circuit of the 3D Trojan is placed in tier 1 while the payload circuit is located near the Trojan target. This type of 3D Trojans is similar with the 2D Trojans that are triggered by an external signal. For instance, the work [26] demonstrates an external probe sensor that initiates the Trojan by manipulating the ring oscillator and LC coil. As the emerging of heterogeneous 3D integration, the external trigger can be originated from the other tiers. Since the payload circuit is never or rarely enabled without the valid cross-tier

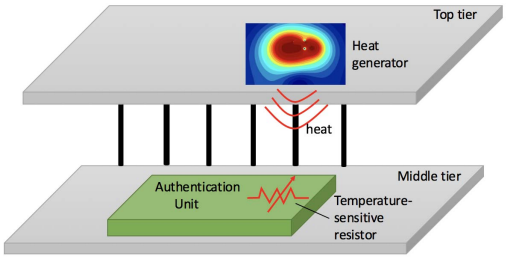

Fig. 3. Temperature triggered cross-tier Trojan.

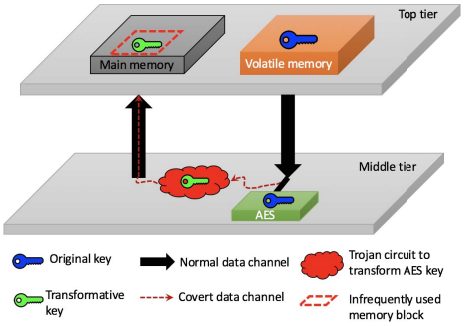

Fig. 4. Key leaking in stacked 3D structure.

trigger signal, the symptom of the target under Trojan attack will not be observed. Thus, this type of Trojans is stealthy. We illustrate the case 1 Trojan with an example shown in Fig. 3. The trigger circuit is a heat generator in the top tier. The payload circuit is a temperature sensitive resistor, which is built in the authentication unit in the middle tier. When the heat from the top tier is passed to the middle tier, the temperature-sensitive resistor could alter the delay of the critical path or cause timing violations, thus resulting in a malfunction of the authentication unit.

B. Cross-Tier Trojan Payload

In the case 2 shown in Fig. 2, the payload of a stealthy 3D Trojan is located in the top tier (tier 1), from where it is relatively easier to probe and measure side-channel signals than from the middle tier(s). The motivation of this type of 3D Trojans is to snoop the confidential information from the victim unit (e.g. crypto engine). As the payload resides in another tier, the effect of this kind of Trojan will not be observable when we do tier-level testing. Here, we assume that the trigger circuit is small enough to hide its area, delay and power overhead. This assumption is as reasonable as what we usually have in 2D ICs. The victim unit in the example shown in Fig. 4 is an AES encryption module. The crypto key is loaded from the volatile memory in tier 1. The purpose of this Trojan is to leak the crypto key. To prevent the key leakage from being captured during the tier 2 testing, the snooped key is transformed into another format (i.e., obfuscated key), and then the Trojan passes the obfuscated key to the rarely used main memory in tier 1. When we test tier 1, the main memory function is normal. As a result, the separated testing on tiers 1 and 2 will not reveal the presence of the 3D Trojan. However, the key will be leaked by the covert channel built by the cross-tier 3D Trojan.

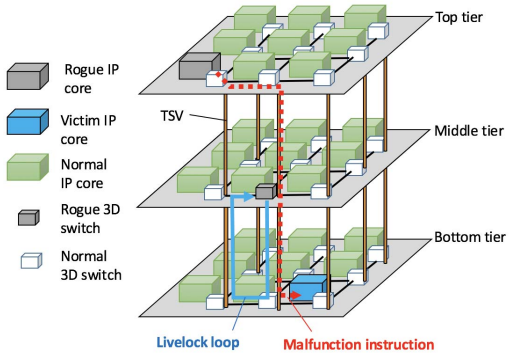

Fig. 5. Cross-tier collaborative hardware Trojan causing livelock and malfunction.

C. Multi-Tier Collaborative Trojan Trigger

The cross-tier hardware Trojan in case 3 shown in Fig. 2 is activated by the two trigger circuits from tiers 1 and 2, respectively. Compared to hardware Trojans in 2D ICs, this type of cross-tier hardware Trojan may have significantly lower Trojan triggering probability due to a larger pool of trigger signals. Similar with the example mentioned in Section IV-A, the collaborative Trojan trigger could be a combination of different trigger mechanisms (e.g., temperature, voltage level, and electromagnetic flux). Alternatively, the trigger circuits are composed of multiple portions, which are distributed in multiple tiers.

3D network-on-chip (NoC) [27], [28] has been demonstrated as a promising infrastructure to integrate increasing transistors in multiple tiers. 3D NoC eliminates the need for long global interconnects and reduces the voltage droop and power consumption on long wires. A rogue 2D NoC leads to information leaking and bandwidth depletion [29]. If NoC based 3D ICs have a collaborative Trojan placed in the IP core and 3D switch, that Trojan leads to the similar consequence, as shown in Fig. 5. The rogue IP core sends a NoC instruction packet to the rogue switch. Next, the rogue switch passes that malicious packet to the victim IP core in the bottom tier. As a result, the multi-tier collaborative Trojan eventually causes the victim IP core having malfunctions. Or, the rogue switch in the middle tier could trigger a livelock between the middle and bottom tiers. The proposed multi-tier collaborative Trojan is stealthy because the hardware of the rogue IP core and switch has high similarity with the normal ones and the 'rogue' feature is only visible at the arrival time of special NoC packets.

D. Information Leaking in Passive Layer

In the case 4 shown in Fig. 2, the Trojan circuit snoops the data (or even the side-channel signal) available in the middle tier. Thanks to the vertical integration of heterogeneous tiers, it is much easier to implement the snooping attack in a malicious tier. Compared with 2D chips, a thin malicious tier provides better flexibility and control on the snooped

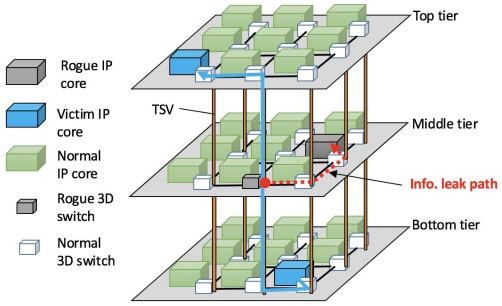

Fig. 6. Cross-tier collaborative hardware Trojan causing information leaking.

information. As envisioned in the work [23], a Trojan tier could observe the information passing between tiers without leading to noticeable delay overhead. Figure 6 illustrates a practical example for the case 4 Trojan model. As shown, the rogue switch and IP core monitor the special packet transversing through the middle tier and the packet of interest in the rogue IP core is stored for future use and analysis. The Trojan type proposed in this subsection is non-invasive, as the Trojan does not alter the normal operation and communication of the system. Moreover, the snooping attack is hidden in the normal data transmission of the middle tier. Side-channel analysis on the entire system may not be able to detect the presence of such hardware Trojan.

V. Experimental Verification on Thermal Trojan

A case study on the thermal-triggered Trojan shown in Fig. 3 is performed in this section. We performed a case study on a platform composed of Xilinx Nexys3 Spartan-6 FPGA, TI MSP430FR6989 LauchPad borad, IRF540 MOSFET transistor, and NTC thermistor. The purpose of this case study is to verify the implementation feasibility of the thermal Trojan and compare its activation efficiency between the scenarios of 2D and 3D ICs.

A. Experimental Setup

In the experiment below, we demonstrate how an attacker uses thermal-triggered Trojan to compromise the authentication system. The overview of our experimental setup is shown in Fig. 7. The two isolated blocks in the breadboard are used to mimic two adjacent tiers in a 3D IC. A heat generator circuit and a thermal sensing circuit are implemented in the two blocks, respectively. The main component of the heat generator circuit is a MOSFET driven by the FPGA board shown Fig. 7. The sensor circuit composed of a NTC thermistor connected with multiple resistors in series is powered by the TI microcontroller shown in Fig. 7. When the thermistor senses temperature rising, its resistance starts to drop, which leads to a decrease on its voltage level. To simulate the 2D scenario for comparison, we add a heat sink for the heat generator circuit, as shown in Fig. 8, to provide a better heat dissipation which is commonly provided in 2D IC.

A Trojan trigger logic is programmed in the FPGA to monitor two input signals, which are controlled by the two switches. An authentication system is programmed in the

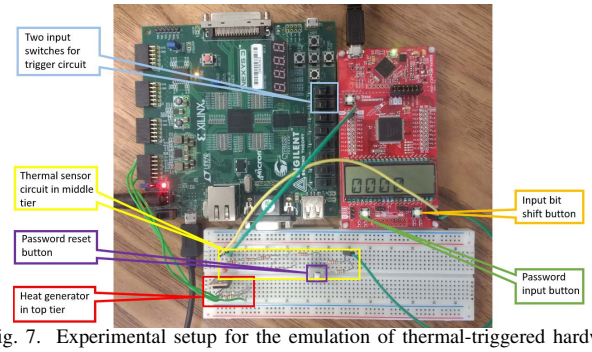

Fig. 7. Experimental setup for the emulation of thermal-triggered hardware Trojan in 3D ICs.

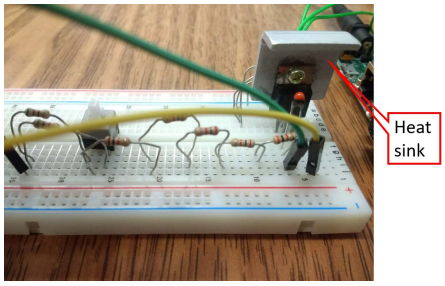

Fig. 8. Implementation of heat sink.

microcontroller to examine the password provided externally. The microcontroller also detects the voltage level of the thermistor. The triggered Trojan turns on the MOSFET (thus it starts to burn) to heat the temperature in the surrounding area. Once the thermistor senses the temperature increasing, then the microcontroller detects the change on voltage and drives the authentication system jump to the password reset status. We successfully mimicked a 3D thermal-triggered hardware Trojan and overwrote the authentication password.

B. Trojan Activation Efficiency

In this subsection, we compare the activation speed of the thermal-triggered Trojans emulated for 2D and 3D scenarios. We used the microcontroller to implement a threshold comparator to examine the voltage level of the thermistor. If the voltage of thermistor exceeds the threshold, the Trojan payload will reset the authentication password. The trigger of our Trojan is thermal effect. We warmed the air surrounding the thermistor with and without the heat sink to mimic 2D and 3D scenarios, respectively. Then, we measured the time that the thermistor takes to drop the voltage below the threshold for each case. The results are shown in Table II. In the 2D scenario, the Trojan needs almost twice of the time to be activated compared to the 3D scenario. Due to the poor heat dissipation, it is easier to implement thermal-triggered Trojans in 3D ICs. We also measured the temperature changing within 12 minutes for each scenario. The changing speed is reflected by the resistance of thermistor. The dropping trend of the resistance is plotted in Fig. 9. As can be seen, the NTC thermistor's resistance for the 3D case drops faster than that for the 2D case. This fact further confirms that heat can be better accumulated in 3D than 2D and 3D ICs will facilitate the implementation of thermal-based Trojans.

TABLE II
TROJAN ACTIVATION EFFICIENCY

Emulation scenarios	Time to trigger Trojan (min)
2D	11:12
3D	6:52

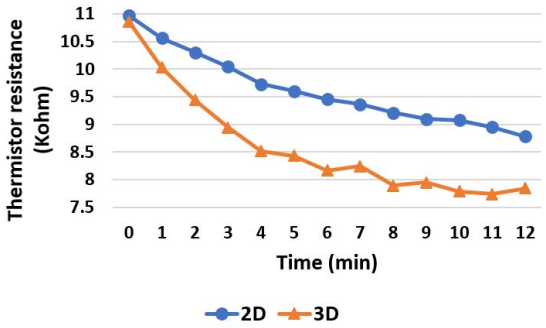

Fig. 9. Speed of thermistor resistance dropping.

VI. CONCLUSION

Vertical integration of multiple dies into a single packet potentially leaves more exploration space for attackers to insert stealthy hardware Trojans. Due to the limited testing techniques for 3D ICs, the hardware Trojans in 3D ICs are not easy to detect. In this work, we propose four 3D hardware Trojan models, which are unique for 3D ICs. We provide a practical implementation for each proposed Trojan model and analyze its stealthiness. FPGA and microcontroller based platform is developed in this work to emulate the thermal-triggered hardware Trojan in 3D ICs. Our experimental results show that 3D Trojan can be successfullly triggered with a faster speed than 2D ones.

ACKNOWLEDGEMENT

This work was supported in part by Semiconductor Research Corporation (SRC) and National Science Foundation award No.1717130.

REFERENCES

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

[2] L. Xue, C. C. Liu, H.-S. Kim, S. K. Kim, and S. Tiwari, "Three-dimensional integration: Technology, use, and issues for mixed-signal applications," *IEEE Transactions on Electron Devices*, vol. 50, pp. 601–609, March 2003.

[3] J. Dofe, Q. Yu, H. Wang, and E. Salman, "Hardware security threats and potential countermeasures in emerging 3D ICs," in *Proc. GLSVLSI'16*, pp. 69–74, ACM, 2016.

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

[5] Y. Xie, C. Bao, C. Serafy, T. Lu, A. Srivastava, and M. Tehranipoor, "Security and Vulnerability Implications of 3D ICs," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 2, pp. 108–122, April 2016.

[6] D. Juan, S. Garg, and D. Marculescu, "Statistical thermal evaluation and mitigation techniques for 3d chip-multiprocessors in the presence of process variations," in *Proc. DATE'11*, pp. 1–6, March 2011.

[7] S. Garg and D. Marculescu, "System-level process variability analysis and mitigation for 3d mpsocs," in *Proc. DATE'09*, pp. 604–609, April 2009.

[8] Y. Alkabani and F. Koushanfar, "Extended abstract: Designers hardware trojan horse," in *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, pp. 82–83, June 2008.

[9] Z. Zhang and L. Njilla and C. A. Kamhoua and Q. Yu, "Thwarting Security Threats From Malicious FPGA Tools With Novel FPGA-Oriented Moving Target Defense," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, pp. 665–678, March 2019.

[10] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Design Test of Computers*, vol. 27, pp. 10–25, Jan 2010.

[11] K. Xiao, D. Forte, and M. Tehranipoor, "A novel built-in self-authentication technique to prevent inserting hardware trojans," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 33, pp. 1778–1791, Dec 2014.

[12] S. Moein, T. A. Gulliver, F. Gebali, and A. Alkandari, "A new characterization of hardware trojans," *IEEE Access*, vol. 4, pp. 2721–2731, 2016.

[13] T. Inoue, K. Hasegawa, M. Yanagisawa, and N. Togawa, "Designing hardware trojans and their detection based on a svm-based approach," in *Proc. ASICON'17*, pp. 811–814, Oct 2017.

[14] G. T. Becker, F. Regazzoni, C. Paar, and W. P. Burleson, "Stealthy dopant-level hardware trojans," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 197–214, Springer, 2013.

[15] R. Kumar, P. Jovanovic, W. Burleson, and I. Polian, "Parametric trojans for fault-injection attacks on cryptographic hardware," in *2014 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pp. 18–28, Sept 2014.

[16] D. Hly, M. Augagneur, Y. Clauzel, and J. Dubeuf, "Malicious key emission via hardware trojan against encryption system," in *Proc. ICCD'12*, pp. 127–130, Sept 2012.

[17] N. Hu, M. Ye, and S. Wei, "Surviving information leakage hardware trojan attacks using hardware isolation," *IEEE Transactions on Emerging Topics in Computing*, pp. 1–1, 2018.

[18] N. Fern, I. San, . K. Ko, and K. T. Cheng, "Hiding hardware trojan communication channels in partially specified soc bus functionality," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 36, pp. 1435–1444, Sept 2017.

[19] S. F. Mossa, S. R. Hasan, and O. Elkeelany, "Hardware trojans in 3-d ics due to nbti effects and countermeasure," *Integration*, vol. 59, pp. 64–74, 2017.

[20] S. R. Hasan, S. F. Mossa, O. S. A. Elkeelany, and F. Awwad, "Tenacious hardware trojans due to high temperature in middle tiers of 3-d ics," in *2015 IEEE 58th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 1–4, Aug 2015.

[21] J. Dofe, P. Gu, D. Stow, Q. Yu, E. Kursun, and Y. Xie, "Security threats and countermeasures in three-dimensional integrated circuits," in *Proceedings of the on Great Lakes Symposium on VLSI 2017*, pp. 321–326, ACM, 2017.

[22] S. Madani and M. Bayoumi, "A security-aware pre-partitioning technique for 3d integrated circuits," in *Proc. MTV'17*, pp. 57–61, Dec 2017.

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

[24] S. Madani, M. R. Madani, I. K. Dutta, Y. Joshi, and M. Bayoumi, "A hardware obfuscation technique for manufacturing a secure 3D IC," in *Proc. MWSCAS'18*, pp. 318–323, Aug 2018.

[25] P. Yang and M. Marek-Sadowska, "Making split-fabrication more secure," in *2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pp. 1–8, Nov 2016.

[26] X. T. Ngo, Z. Najm, S. Bhasin, D. B. Roy, J.-L. Danger, and S. Guilley, "Integrated Sensor: A Backdoor for Hardware Trojan Insertions?," *in Proc. 2015 Euromicro Conference on Digital System Design*, pp. 415–422, 2015.

[27] M. H. Jabbar, D. Houzet, and O. Hammami, "3D multiprocessor with 3D NoC architecture based on Tezzaron technology," in *Proc. of 3DIC '11*, pp. 1–5, Jan 2012.

[28] L. Jiang and Q. Xu, "Fault-Tolerant 3D-NoC Architecture and Design: Recent Advances and Challenges," in *Proc. of NOCS '15*, pp. 7:1–7:8, 2015.

[29] J. Frey and Q. Yu, "A hardened network-on-chip design using runtime hardware Trojan mitigation methods," *Integration, the VLSI Journal*, vol. 56, pp. 15 – 31, 2017.