Analysis of the Security Vulnerabilities of 2.5-D and 3-D Integrated Circuits

Vaibhav Venugopal Rao
Drexel University
Philadelphia, Pennslyvania 19104
Email: vv85@drexel.edu

Avesta Sasan
University of California, Davis
Davis, California 95616
Email: asasan@ucdavis.edu

Ioannis Savidis
Drexel University
Philadelphia, Pennslyvania 19104
Email: isavidis@coe.drexel.edu

***Abstract*—The need for greater functionality on a single integrated circuit (IC) has directly resulted in novel techniques, methodologies, and processes that increase device density. In addition to device density, the advent of 2.5-D and 3-D integration has allowed for the development of complex heterogeneous systems, where intellectual property (IP) across multiple vendors and from different process nodes and foundries are placed in close proximity. Although 2.5-D and 3-D integration opens the door to enhanced circuit functionality, the physical security of such systems, which was already a challenge with 2-D integrated circuits, is of greater concern. The potential for sourcing and integrating adversarial IP including hardware Trojans, placing untrusted ICs, leaking critical circuit functionality or user data through side-channels, or even allowing for attack through the exploitation of side-channels must be considered. In this paper, a thorough analysis of the security vulnerabilities of 2.5-D and 3-D integrated circuits to Trojan insertion and side-channel attack is provided, with the goal of highlighting the importance of considering the security implications of such systems during design.**

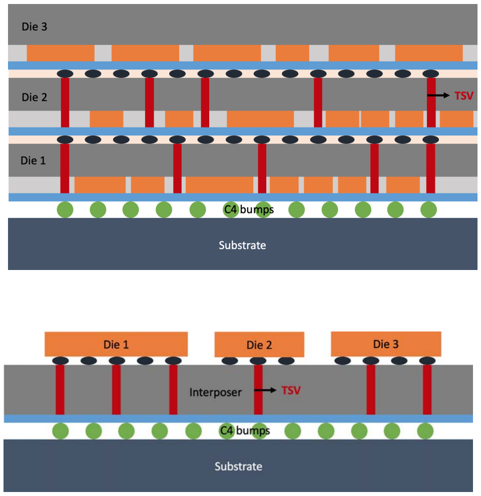

Fig. 1: Vertical cross-sections of a (a) stacked 3-D IC and (b) interposer-based 2.5-D IC.

I. Introduction

Technology scaling has been the impetus for the advancement of smaller, faster, and more efficient integrated circuits with increased functionality. However, technology scaling has been hindered by increasing physical, material, power, thermal, and economic challenges, including from limitations due to short channel effects, leakage currents, and the management of variability [1]. To address the limitations of technology scaling, the utilization of the vertical dimension for the implementation of an integrated circuit provides a suitable solution. Recent work by academic, commercial, and government organizations implementing 2.5-D and 3-D ICs have demonstrated systems with superior performance, higher memory bandwidths, greater energy efficiencies, smaller form factors, and heterogeneously integrated components [2], [3].

The utilization of 2.5-D and 3-D integration allows for the vertical stacking of functional transistor layers that are interconnected through microbumps or through-silicon-vias (TSVs) as shown in Fig. 1. For 3-D integrated circuits, multiple dies (homogeneous and/or heterogeneous) are stacked one on top of the other while utilizing TSVs for high-bandwidth signaling [4], [5]. Vertically stacking dies to form a 3-D IC provides for increased device density and reduced interconnect length, which correspondingly reduces power consumption and delay [6]. For 2.5-D integrated circuits, multiple dies are placed side-by-side on an interposer (typically made of silicon) that provides interconnects for inter-die communication. The interposer also provides an interface between the dies and the input and output (I/O) ports of the package through TSVs that traverse the substrate. The interposer, therefore, serves as a high-bandwidth and low latency communication interface in addition to allowing for the global distribution of power and clock signals [7].

Due to the globalization of the IC supply chain, there is increased concern in hardware related vulnerabilities that include IP piracy, counterfeiting, overproduction, reverse engineering, and side channel attacks [8]. The concern over vulnerabilities in the IC supply chain has resulted in novel research in techniques and methodologies that secure the circuit during the design, fabrication, test, and in-field use of the device. However, security-aware hardware design results in considerable overhead in area and degrades the performance of the circuit as additional security related components are integrated within the die. With the recent advances in 2.5-D and 3-D integration, there is an opportunity to improve existing countermeasures through the addition of security features without impacting the overall performance of the stacked system [6]. Although 2.5-D and 3-D technologies provide security advantages, such circuits also suffer from unique vulnerabilities that differ from traditional 2-D ICs. Understanding the security vulnerabilities unique to 2.5-D and 3-D ICs is critical in the development of robust security methodologies needed for such circuits, which is, therefore, the focus of this paper.

978-1-6654-9466-3/22/$31.00 ©2022 IEEE

The paper is organized as follows. A brief discussion on the unique security challenges in the design, testing, and operation of a 2.5-D and 3-D integrated circuit is provided in Section II. Existing work on hardware Trojans that target 2.5-D and 3-D ICs is discussed in Section III. Vulnerabilities of the 2.5-D and 3-D ICs to thermal and power-based side-channel attacks are described in Section IV. Concluding remarks are provided in Section V.

II. Security Vulnerabilities

Although 2.5-D and 3-D technologies provide security advantages, there are also unique vulnerabilities that must be considered, where security techniques developed for 2-D ICs are not directly applicable. The increased device density and functionality has resulted in greater sophistication, time, and cost needed for testing the ICs. Although each die and corresponding TSVs are tested during the pre- and mid-bond stages, testing of die-to-die vertical communication channels is hindered by the limited access to test nodes. In addition, the use of standard testing probes risks damaging the TSVs, which is of concern as the reliability of the circuit is dependant on TSVs that meet target electrical specifications [9]. The challenges in the functional testing of 2.5-D and 3-D ICs limit the probability of detecting a malicious component(s) in the stacked system.

Both 2.5-D and 3-D ICs suffer from greater variation in process, voltage, and temperature (PVT) as compared to 2-D ICs, where the temperature for a 4-tier 3-D IC is as much as 40x higher than that of a single tier 2-D IC [10]. The large variations not only increase the cost of detecting hardware Trojans using side-channel analysis during test but also increase the corresponding risk of leaking information through the power and thermal side channels. The large number of switching devices, the increased thermal gradients, and the greater PVT variations mask the activation and trigger mechanisms of hardware Trojans and reduce the probability of detection during testing. In addition, the large leakage noise associated with 2.5-D and 3-D ICs effectively masks the leakage of critical information through hardware Trojans or side-channels. The unique vulnerabilities of 2.5-D and 3-D technologies to hardware Trojans and side-channel analysis are discussed in Sections III and IV, respectively.

III. Hardware Trojans

Hardware Trojans are intentional and malicious modifications to the original IC that alter the functionality of the circuit or leak critical information. Depending on the activation mechanism, Trojans are classified as internally or externally triggered [11]. Based on the trigger mechanism, Trojans are further classified as i) always on, ii) combination logic triggered, or iii) sequentially triggered. When the trigger conditions are met, the Trojan is activated and executes pre-set malicious operations that range from transmitting critical information to degrading the circuit performance.

Significant prior research in the development of 2-D Trojan models has facilitated greater understanding of 2-D Trojan placement, trigger mechanisms, and execution, which resulted in robust Trojan detection and prevention methodologies [11]. However, the lack of 2.5-D and 3-D Trojan models has limited the development of Trojan detection methodologies. In addition to the increased vulnerability of 2.5-D and 3-D technologies to Trojan insertion during the design and fabrication phase, the stacking of multiple device planes offers another dimension for the attackers to insert hardware Trojans. Split manufacturing has been proposed to mitigate reverse engineering and Trojan insertion in 3-D ICs [6]; however, recent advances in electronic design automation (EDA) tools have minimized the security advantages provided by split manufacturing as an attacker is able to exploit the structured results produced by placement and routing algorithms to perform proximity attacks [12]. The split manufacturing process, the stacking of multiple dies, the TSVs, and the increased PVT variations of 2.5-D and 3-D ICs have allowed for novel hardware Trojans with characteristics (i.e. placement, trigger mechanisms, and payloads) that differ from Trojans implemented in 2-D circuits. Therefore, existing 2-D Trojan detection methodologies are not directly applicable to 2.5-D and 3-D ICs.

The increase in device density and the number of tiers stacked to form a 3-D IC, coupled with the cost in area and complexity in designing heat removal capabilities, has resulted in increased thermal challenges. Poor thermal management, and the corresponding detrimental effects that include accelerated aging and increased variations, has resulted in a greater number of Trojans that exploit the thermal characteristics of 2.5-D and 3-D ICs. Therefore, in this paper, 2.5-D and 3-D Trojans are classified as either thermal-activated or non-thermal activated.

A. *Thermal-activated Trojans*

The thermal-activated Trojans exploit the poor heat dissipation of 3-D ICs as a trigger mechanism. The generation and accumulation of heat in the IC alters the electrical parameters of the transistors and the switching speeds of the gates over a period of time, which results in an increase in transitions to unspecified FSM states and glitches. The 2.5-D and 3-D Trojans exploit unspecified state transitions and glitches as trigger mechanisms, which removes the need for an explicit trigger circuit, and, therefore, reduces the probability of detecting the Trojan during testing [11].

In 2.5-D and 3-D ICs, the trigger mechanisms and payload components of the Trojans are potentially separated into multiple tiers. In addition, the implementation of trigger mechanisms that are split and located across multiple tiers and that jointly activate a Trojan payload are possible. Based on the trigger mechanisms and/or location of the Trojan payload, the thermal-activated Trojans are further classified as either TSV/interposer located Trojans or cross-tier located Trojans.

1) TSV/Interposer located Trojans: TSV/Interposer located Trojans exploit the TSV structure of a 3-D IC or the TSV and interposer structure of a 2.5-D IC to trigger the execution of malicious functionalities in the IC. The Trojans proposed in [13], exploit both the thermal characteristics and the TSV structure of 2.5-D and 3-D ICs for Trojan activation that results in a denial-of-service (DoS) attack. The threat model assumed for the Trojans described in [13] is that of an untrusted interconnect facility or integration facility and an untrusted single die fabrication facility, where the attacker possesses the circuit information in the form of a geometric data stream for information interchange (GDSII file). The Trojan proposed in [13] consists of only a single transistor switch between two TSVs. The Trojan is activated through a thermal sensor, where for specific temperatures, the transistor switch turns on and creates a short circuit between the two TSVs that results in a denial-of-service. A Trojan based on an aging accelerator is also proposed in [13]. Resistive based heat generation units are used to accelerate the aging of the circuit, which results in aging induced metal disconnect in the TSVs or interconnects and threshold voltage shifting in the transistors, leading to poor reliability over time.

2) Cross-tier located Trojans: The Trojans that have trigger mechanisms and/or payloads spread across multiple dies of a 2.5-D and 3-D IC are classified as cross-tier Trojans. The cross-tier Trojans are not detected during the functional test of each individual tier as the trigger mechanism requires the connection of the Trojan components found across multiple device planes.

The Trojans proposed in [14], [15] assume an untrusted foundry, where the attacker has access to the GDSII files. The Trojan exploits the negative bias temperature instability (NBTI) aggravated by the thermal characteristics of the 3-D ICs. NBTI degrades the electrical parameters of the transistor including the switching time, drain current, and threshold voltage. The temporary timing glitches caused by NBTI are exploited for Trojan activation in a 3-D IC without the need for additional trigger circuitry. The Trojan circuit consists of the undesired states of the finite state machine (FSM) of a 3-D IC in one of the device planes and the momentary glitch caused by NBTI, which activates the Trojan and transitions the circuit into an undesired state. The undesired state either causes a denial of service or leaks critical information from the circuit. The traditional fault-tolerant based testing applied to 2-D ICs does not accurately predict or model the temperature gradients in the different tiers of a 3-D IC, which results in a decrease in the probability of activating and detecting the Trojan during test. In addition, the presence of Trojans in the middle tiers of a 3-D stack not only aggravates the effect of NBTI due to the poor thermal properties of a 3-D IC but also increases the difficulty of detecting the Trojans [15].

B. Non-Thermal Activated Trojans

Trojans that do not exploit the thermal properties of 2.5-D and 3-D ICs are classified as non-thermal activated Trojans. Similar to the thermal activated Trojans discussed in III-A, non-thermal activated Trojans are classified as either TSV/interposer located Trojans or cross-tier located Trojans.

1) TSV/Interposer located Trojans: Both inter-die signals and power delivery networks are routed between multiple dies or the interposer through TSVs. A 2.5-D and 3-D integration facility that manufactures the TSVs possesses the necessary skills and tools needed to introduce hardware Trojans into the TSV structure that potentially results in side-channel leakage and/or poor signal integrity and circuit reliability. The limited testing capability post bonding further reduces the probability of detecting the TSV based Trojans during functional test. Based on the TSVs used for routing power and signals, the Trojans are further classified into either power-TSV based Trojans or signal-TSV based Trojans, respectively [16].

The power-TSV based Trojans proposed in [16] exploit the electrical properties of the TSVs to weaken the reliability of the victim IC. The proposed Trojan is placed in the TSVs of a Via-First bonding process that is completed during fabrication of the front-end of the line (FEOL). The Via-First TSVs provide power and ground connections between the top and bottom tiers of a stacked IC. An untrusted interconnect facility is assumed, where the attacker has access to the GDSII files. A typical TSV is modeled using a series resistor and inductor along with a parallel capacitor, whose values depend on the length, thickness, and material composition of the TSVs [21]. The proposed power-TSV based Trojans modify the per-unit length resistance of the TSVs, which affects both the peak power and the gate delay by either changing the chemical composition or altering the physical dimensions of the TSVs [16]. The analysis of the effect of the proposed Trojan on an inverter in the bottom tier of a two-tiered stack resulted in a 15% reduction in the peak power and an 11% increase in the inverter delay, which is significant enough to cause timing errors in the IC [16]. In addition, the reduction in the effective resistance of the TSVs results in a corresponding increase in the current density, which leads to electromigration and accelerated device aging. Accelerated device aging affects the reliability and signal integrity of the circuit, which act as trigger mechanisms for the type of Trojans proposed in [14] and [15].

Similar to the power-TSV based Trojans, the signal-TSV based Trojans exploit the electrical properties of the TSVs to detrimentally affect the reliability of the victim IC [16]. The signal-TSVs are routed through both the silicon substrate and the on-die metalization layers, which exposes a critical and large design space to Trojan insertion. The proposed signal-TSV based Trojans assumes an untrusted interconnect facility, where the attacker has access to the GDSII files. The Trojan modifies both the effective resistance and capacitance of the TSVs, which affects the interconnect delay between a given input signal and the corresponding output node. The activation of a signal-based TSV Trojan located between two inverters placed on separate tiers resulted in an approximately 90 ps increase in the delay for a 100 fF change in the effective capacitance of the TSV. The peak power of the load inverter also increased by 2x with the increase in the effective capacitance of the TSV. The significant increase in the delay resulted in timing errors [16]. In addition, by increasing the effective inductance of the TSV, either by changing the chemical composition or by altering the dimensions of the

TABLE I: Summary of hardware Trojans targeting 2.5-D and 3-D ICs.

Trojan Type	**Trojan Location**	**Paper**	**Threat Model**	**Trojan Information**		
				Trigger	**Characteristics**	**Consequences**
Thermal	**TSV/ Interposer**	[13]	- Untrusted TSV fabrication facility - Untrusted die fabrication facility	Thermal sensors	Short between TSVs	- DoS
	Cross-tier	[14]	- Untrusted die fabrication facility	Timing glitches due to NBTI	Enter undesired FSM states	- DoS - Information leakage
		[15]	- Untrusted die fabrication facility	No specific triggers	- Trojan in middle tier - Hard to detect and probe	- DoS - Information leakage
Non-Thermal	**TSV/ Interposer**	[16]	- Untrusted TSV fabrication facility	Alters the effective resistance of TSVs	- Affects power TSVs - Changes peak power and delay of gates	- Timing violations - Reduced reliability
		This paper	- Untrusted TSV fabrication facility	Alters the effective resistance of TSVs	- Affects power TSVs - Increases electromigration - Accelerated device aging	- Reduced reliability
		[16]	- Untrusted TSV fabrication facility	Alters the effective resistance and capacitance of TSVs	- Affects signal TSVs - Alters interconnect delay	- Timing violations
		This paper	- Untrusted TSV fabrication facility	Alters the effective inductance of TSVs	- Affects signal TSVs - Increases EM radiation	- Information leakage
	Cross-tier	[17]	- Untrusted die fabrication facility	Uses TSVs to access different tier	Trojan snoops/alters the functionality of IP in another tier	- DoS - Information leakage
		[18]	- Untrusted assembly facility	Placement of additional Trojan tier	- Extract information via TSVs - Controller disturbs operation	- DoS - Information leakage
		[19]	- Untrusted die fabrication facility	No specific triggers	Target voids in the IC for Trojan placement	- DoS - Information leakage
		[20]	- Untrusted die fabrication facility	Heat generator in top tier	Thermistor alters the delay of critical path	- Timing violations
		[20]	- Untrusted die fabrication facility	No specific trigger	Facilitates easy probing and/or measurement of side-channel signals	- Information leakage
		[20]	- Untrusted die fabrication facilities	NoC packets from malicious IP	NoC instructions from malicious IP affects victim IP in different tier	- IC malfunction
		[20]	- Untrusted die fabrication facilities	Placement of additional Trojan tier	IP and switches in Trojan tier monitor exchanges of packets	- Information leakage

TSV, an increase in the electro-magnetic (EM) radiation of the IC was observed. The increase in the EM radiation results in greater likelihood of side-channel attacks, where the critical signals of a circuit are routed through signal-based TSV Trojans to emit EM radiation.

2) Cross-tier located Trojans: In cross-tier located Trojans, either the Trojan payload(s) or the trigger mechanism(s) are spread across multiple-dies. The work in [17] proposes a cross-tier Trojan, where the Trojan payload located in one tier leaks encryption data from another tier. An untrusted single die fabrication facility is assumed, where the attacker has access to the GDSII files [17]. By implementing the proximity attack, the attacker determines the critical information on the interconnects and on different tiers, which allows for the better design and placement of Trojans [12]. Split manufacturing was considered a viable option to thwart hardware security attacks including the insertion of Trojans; however, a sub-optimized partitioning of the device planes compromises the security of the entire 2.5-D and 3-D IC. The hardware Trojan in one tier has the potential to access information or circuit functionality in another tier even when the target tier is secured, which leads to leakage of critical information or denial-of-service. The signal-TSVs are routed through the silicon substrate and the metalization layers of the encrypted die, where a Trojan present in another die utilizes the TSVs to snoop on critical information including the encryption keys or alter the functionality of the encrypted die.

The work described in [18] proposes the placement of an additional dedicated device plane in the 3-D IC stack for Trojan insertion without the knowledge of the IC owner. The work in [18] assumes an untrusted assembly facility, where the attacker has GDSII information and the locations of the TSVs. The proposed Trojan die is placed between two critical dies, while also containing memory elements to extract and store critical information determined from signals propagating on the TSVs. In addition, the extra die also contains hidden controllers to either interrupt the normal functionality of the IC or to cause a denial-of-service. The increased PVT variations due to the stacking of multiple dies in a 3-D IC reduces the probability of detecting the extra device plane, as the additional delay induced by the adversarial tier is challenging to differentiate.

The regions of the die that include decoupling capacitors or empty regions that account for thermal, signal integrity, and design rule requirements are targeted for Trojan insertion in [19]. An untrusted fabrication facility is assumed, where the attacker has access to the GDSII files of the target die. The inserted Trojans degrade the overall circuit performance, create a backdoor for remote control of the IC, or add additional hidden functionalities to increase the leakage of critical information. In addition, similar to [18], neighboring die fabricated in trusted foundries that include security features are also targeted by the proposed Trojan.

In [20], four different Trojans are proposed that target 2.5-D and 3-D ICs based on the position of the Trojan payloads and the trigger mechanisms that activate the Trojans. The four Trojans include 1) a cross-tier trigger, 2) a cross-tier payload, 3) a multi-tier collaborative trigger, and 4) a payload that permits information leakage from a passive layer. An untrusted foundry is assumed, where the attacker possesses the GDSII files. For the cross-tier Trojan trigger, the trigger mechanism is placed in one tier, while the Trojan payload is located on another tier. A Trojan that consists of a heat generator and a thermistor-based payload circuit is proposed in [20]. When the Trojan trigger conditions are met, the thermistor-based Trojan is activated, which modifies the delay of the critical paths and leads to timing violations.

A cross-tier Trojan payload is placed in the top device plane of a 3-D IC, which facilitates easy probing and measurement of side-channel signals. In [20], the secret crypto-key of the AES encryption algorithm implemented in the middle tier of a 3-D IC is leaked through the analysis of the thermal and EM side-channels.

The multi-tier collaborative trigger proposed in [20] consists of a cross-tier Trojan that is activated by trigger circuits found on multiple tiers. A Trojan placed in the 3-D network-on-chip of a 3-D IC is proposed, where a collaborative Trojan is placed in the IP cores and the switching circuit. The malicious IP in one tier sends NoC instructions to a victim core in a different tier through a malicious switch, resulting in errors in the victim core. The proposed Trojan evades detection during testing as the trigger mechanism is only observable during the arrival time of the trigger packets on the NoC.

The leaked information through the passive layer proposed in [20] is similar to the dedicated Trojan tier described in [18]. The Trojan tier consists of a malicious IP core and switches that monitor the exchange of packets traversing through the middle tier. The packets of interest are stored in the memory elements of the Trojan tier for further analysis. A snooping attack is masked within the normal data transmission between device planes. Therefore, the detection of the attack through side channel analysis is a challenge.

Existing hardware Trojans that target 2.5-D and 3-D ICs are summarized in Table I. The Trojans are classified based on type (payload and trigger) and placement. A brief summary of the Trojan trigger mechanisms, characteristics unique to 2.5-D and 3-D ICs, and the resulting effects on the circuit from execution of the Trojan payload are also described.

IV. Side-channel Attack

Side-channel attacks (SCA) exploit the intrinsic physical signals produced by an IC through normal execution. Side-channels include the power consumption, delay, thermal profile, and emanating EM radiation, all of which are utilized to retrieve the critical functionality and operating information of an IC. In recent years, SCA has been shown to effectively determine the secret key of cryptographic circuits or reduce the key-space during a satisfiability or brute-force attack [27]. While a large body of research on both the modeling of side-channels and the subsequent developed countermeasures is available for 2-D ICs, similar research for 2.5-D and 3-D ICs is still in an early stage. In addition, the side-channel characteristics of 2.5-D and 3-D ICs differ from that of 2-D ICs. Therefore, the models and the countermeasures developed for 2-D ICs are not directly applicable to 2.5-D and 3-D ICs.

Although the research on the side-channels of 2.5-D and 3-D ICs is limited, there is some early work that describe the vulnerabilities of 2.5-D and 3-D ICs to side-channel attacks. Specifically, the large thermal gradients and the inclusion of Trojans are the two primary sources of side-channel signals in 2.5-D and 3-D ICs, which result in thermal and power-based side-channel attacks, respectively.

A. *Thermal Side Channel Attacks*

The thermal side channel (TSC) attack exploits the infrared (IR) radiation emanating from the IC to determine the functionality of the circuit or decrypt secret information. The TSC attack performed on an Intel Xeon processor, as described in [22], has shown that the execution of an instruction on one core is vulnerable to detection by an adjacent core of a 2-D IC. Extending the same concept to a 2.5-D and 3-D IC, the execution of a cryptographic core in one tier can be captured by a Trojan placed in another tier, where the Trojan enhances the leakage of information by facilitating probing or by amplifying side-channel signals. The TSC attack is successful due to easy access to the functional circuit, the availability of a wide range of thermal Trojans, and the direct correlation of the power side-channel to temperature signals when temperature-to-power interpolation techniques are utilized [23].

The TSC attack proposed in [23], assumes that an attacker has direct physical access to the IC, which allows for the execution of non-invasive attacks. The attacker is also assumed to possess a system level understanding of the IC from the available datasheets. Based on the assumed threat model, two types of TSC attacks are proposed: 1) thermal characterization of the IC and 2) localization and monitoring of modules.

For thermal characterization of an IC, an attacker applies a broad and varied range of input patterns in a step-by-step approach to trigger different activity patterns in the circuit. By monitoring the TSC signals, the attacker builds a model of the thermal behavior of the IC. In addition, the Pearson coefficient [28] of both the power and the thermal profile are developed to accurately predict the password for the security module of the 3-D IC [23].

For the TSC attack that localizes and monitors modules, a given module is targeted by applying specific inputs that activate only select regions of the IC. The specific inputs are determined iteratively by varying the applied inputs and measuring the thermal profile, which is then used to create an input-to-activity mapping file. Once the attacked modules

TABLE II: Summary of side-channel analysis attacks on 2.5-D and 3-D ICs.

SCA Type	Paper	Threat Model		Attack
		Source	Information	Procedure
Thermal-based SCA	[22]	- Untrusted foundry	- GDSII - Oracle IC	Execution of the cryptographic core captured by a Trojan in different tier that leaks side-channel signals
	[23]	- Untrusted end user	- Datasheet - GDSII - Oracle IC	- Model of thermal behavior of the IC determined by mapping input-thermal signatures - PCC to accurately predict the correct key
	[23]	- Untrusted end user	- Datasheet - GDSII - Oracle IC	- Utilize thermal profile to determine inputs for sub-block activation - Encryption modules are localized using specific inputs - PCC to determine the encryption key
	[24]	- Untrusted foundry - Untrusted assembly facility - Untrusted end user	- Datasheet - GDSII - Oracle IC	- Temporal/spatial traces of executing instructions in different functional units - Statistical pattern matching from input-output response and temporal traces to model IC thermal profile - Secret information estimated using generated model
Power-based SCA	[25]	- Untrusted foundry - Untrusted end user	- Oracle IC	- Power consumption of the Sbox for different scenarios of switching and idle tiers are analyzed - PCC between Sbox power consumption of 3-D IC and Sbox power consumption of 2-D IC is calculated - Inputs that localize only the security tier are determined - Correct key is estimated using power traces and statistical pattern matching
	[26]	- Untrusted foundry - Untrusted end user	- GDSII - Oracle IC	- Logic cone extraction - CPA attacks are performed on each logic cone - Real power consumption of all the logic cones is extracted - PCC between the estimated power and real power to determine the correct key for each logic cone

are localized with a certain confidence, secret information is determined by using the Pearson coefficient [28] of the power consumption and thermal profile. Most notably, encryption modules are first localized and then monitored using the signals from the TSC for different input patterns, with the result being an estimate of the value of the encryption keys.

General purpose processors are attacked using the TSC in [24]. Temporal and spatial traces of executing instructions utilizing different functional units produce variations in the thermal profile of the circuit, which are exploited by the attack. The thermal profile produced by specific instructions running on the processor is extracted in one of three ways: 1) built-in thermal sensors in the form of Trojans (non-invasive), 2) external thermal sensors placed by depackaging and attachment of the sensors to various locations on the IC (semi-invasive), and 3) infrared thermal imaging, where the attacker depackages the IC and employs thermal imaging to analyze the thermal profile and spatial distribution of temperature gradients across the IC (semi-invasive). Utilizing the input-output response of the circuit and the TSC traces, accurate models of the IC are constructed by applying statistical pattern matching techniques. Using the generated models, the secret information of the circuit (encryption key) is estimated. Due to the smaller number of active circuit blocks when executing an instruction on a general purpose processor, the correlation of the encryption key to the thermal traces is direct [24].

B. Power-based Side Channel Attack

A power-based SCA exploits the variation in the power consumption of the IC for different execution phases of an application. There are three primary categories of power-based SCA: 1) simple power analysis (SPA), 2) differential power analysis (DPA), and 3) correlation power analysis (CPA).

The CPA is the most advanced form of power SCA that leverages the correlation between the cryptographic key and the switching activity of the crypto-hardware under attack [29]. CPA significantly reduces the execution time of brute-force attacks used to extract the cryptographic key. In [25], the CPA attack is used to determine the correct key applied to an Sbox. Although the number of CPA traces required to determine the correct key applied to an Sbox in a 3-D IC is 1.67x greater than that of a 2-D IC implementation, CPA significantly reduces the key-space to search. In addition, the utilization of a hardware Trojan, as discussed in Section III, greatly increases the signal-to-noise ratio (SNR) of the side-channel signals and further improves the efficacy of the CPA attack. In [25], the power consumption of the Sbox for different scenarios of switching and idle tiers is analyzed. The Pearson correlation coefficients (PCC) between the power consumption for different inputs applied to an Sbox in a 3-D IC and the power consumption for different inputs applied to an Sbox in a 2-D IC are calculated. The scenario that results in the activation of only one tier produces the highest PCC score, which indicates that the 3-D IC produces a similar side-channel response to a 2-D IC for the given applied input pattern. Therefore, by employing the localization and monitoring of modules proposed in [23], the complexity of a power-based SCA attack on a 3-D IC is reduced to that of a power-based SCA attack on a 2-D IC.

In [26], logic-locked monolithic 3-D (M3D) ICs are targeted with a CPA attack. Since the M3D ICs are fabricated using a single foundry unlike TSV-based 3-D ICs, logic locking techniques are employed to increase the security of the circuit [30]. The proposed CPA attack on the logic locked circuits includes four primary steps: 1) logic cone extraction, where all the logic cones of the locked netlist are extracted based on the primary outputs, 2) divide-and-conquer-based power estimation, where CPA attacks are executed on each logic cone based on an ascending order of cone size, 3) power trace collection, where the physical power consumption of all logic cones is extracted for the same input patterns, and 4) correlation analysis, where the PCC between the estimated power consumption determined in step 2 and the real power consumption determined in step 3 is computed to resolve the correct key of each logic cone. The execution of the proposed CPA attack on the c432 benchmark circuit obfuscated with transistor-level camouflaged logic locking [30] resulted in a 100% key retrieval rate with 4000 power traces. The analysis indicates that M3D ICs protected with logic locking techniques are vulnerable to CPA attacks.

The current side-channel attacks that target 2.5-D and 3-D ICs are summarized in Table II. The SCA attacks are categorized into thermal-based and power-based. A brief summary of the SCA attack methodologies is also provided.

V. Conclusions

Advances in 2.5-D and 3-D ICs has allowed for the integration of a greater number of functions with improved efficiency. Although 2.5-D and 3-D technologies provide security advantages, vulnerabilities unique to such circuits exist including Trojan insertion and side-channel attacks. Hardware Trojans implemented in 2.5-D and 3-D ICs are classified as either thermal-activated or non-thermal activated. For both, the TSVs and cross-tier structures are targeted, which is often hard to detect during functional testing. In addition, 2.5-D and 3-D ICs are susceptible to thermal and power-based side channel attacks. A detailed analysis of the different vulnerabilities of 2.5-D and 3-D ICs is provided in this paper, with the goal of enhancing the understanding of various Trojan and side-channel leakage models unique to 2.5-D and 3-D ICs.

References

[1] N. Z. Haron and S. Hamdioui, “Why is CMOS Scaling Coming to an END?,” *Proceedings of the IEEE International Design and Test Workshop*, pp. 98–103, December 2008.

[2] J. Macri, “AMD’s Next Generation GPU and High Bandwidth Memory Architecture: FURY,” *Proceedings of the IEEE Hot Chips Symposium (HCS)*, pp. 1–26, August 2015.

[3] A. Sodani, R. Gramunt, J. Corbal, H.S. Kim, K. Vinod, Sundaram Chinthamani, S. Hutsell, R. Agarwal, and Y.C. Liu, “Knights Landing: Second-Generation Intel Xeon Phi Product,” *Proceedings of the IEEE Micro Journal*, Vol. 36, No. 2, pp. 34–46, April 2016.

[4] V. F. Pavlidis, I. Savidis, and E.G Friedman, “Three-dimensional Integrated Circuit Design (Second Edition),” Morgan Kaufmann, 2017.

[5] I. Savidis and E. G. Friedman, “Closed-Form Expressions of 3-D Via Resistance, Inductance, and Capacitance,” *Proceedings of the IEEE Transactions on Electron Devices*, Vol. 56, No. 9, pp. 1873–1881, August 2009.

[6] S. S. Wong and A. E. Gamal, “The Prospect of 3D-IC,” *Proceedings of the IEEE Custom Integrated Circuits Conference (CICC)*, pp. 445–448, September 2009.

[7] T. G. Lenihan, L. Matthew, and E. J. Vardaman, “Developments in 2.5D: The Role of Silicon Interposers,” *Proceedings of the IEEE Electronics Packaging Technology Conference (EPTC)*, pp. 53–55, February 2013.

[8] M. Rostami, F. Koushanfar, and R. Karri, “A Primer on Hardware Security: Models, Methods, and Metrics,” *Proceedings of the IEEE*, Vol. 102, No. 8, pp. 1283–1295, July 2014.

[9] E. J. Marinissen, “Challenges and Emerging Solutions in Testing TSV-based 2 1 over 2D- and 3D-Stacked ICs,” *Proceedings of the IEEE Design, Automation and Test in Europe Conference and Exhibition (DATE)*, pp. 1277–1282, March 2012.

[10] S. Im and K. Banerjee, “Full Chip Thermal Analysis of Planar (2-D) and Vertically Integrated (3-D) High Performance ICs,” *Proceedings of the IEEE International Electron Devices Meeting*, pp. 727–730, December 2000.

[11] M. Tehranipoor and F. Koushanfar, “A Survey of Hardware Trojan Taxonomy and Detection,” *Proceedings of the IEEE Journal on Design and Test of Computers*, Vol. 27, No. 1, pp. 10–25, February 2010.

[12] S. Chen and R. Vemuri, “Exploiting Proximity Information in a Satisfiability Based Attack Against Split Manufactured Circuits,” *Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 171–180, May 2019.

[13] J. Dofe, Q. Yu, H. Wang, and E. Salman, “Hardware Security Threats and Potential Countermeasures in Emerging 3-D ICs,” *Proceedings of the International Great Lakes Symposium on VLSI (GLSVLSI)*, pp. 69–74, May 2016.

[14] S. F. Mossa, S. R. Hasan, and O. Elkeelany, “Hardware Trojans in 3-D ICs Due to NBTI Effects and Countermeasure,” *Integration, the VLSI Journal*, Vol. 59, No. C, pp. 64–74, September 2017.

[15] 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,” *Proceedings of the IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 1–4, August 2015.

[16] J. Dofe, P. Gu, D. Stow, Q. Yu, E. Kursun, and Y. Xie, “Security Threats and Countermeasures in Three-Dimensional Integrated Circuits,” *Proceedings of the Great Lakes Symposium on VLSI (GLSVLSI)*, pp. 321–326, March 2017.

[17] S. Madani and M. Bayoumi, “A Security-Aware Pre-partitioning Technique for 3-D Integrated Circuits,” *Proceedings of the IEEE International Workshop on Microprocessor and SOC Test and Verification (MTV)*, pp. 57–61, December 2017.

[18] S. Alhelaly, J. Dworak, T. Manikas, P. Gui, K. Nepal, and A. L. Crouch, “Detecting a Trojan Die in 3-D Stacked Integrated Circuits,” *Proceedings of the IEEE North Atlantic Test Workshop (NATW)*, pp. 1–6, May 2017.

[19] Ping-Lin Yang and Malgorzata Marek-Sadowska, “Making Split-Fabrication More Secure,” *Proceedings of the ACM International Conference on Computer-Aided Design (ICCAD)*, pp. 1–8, November 2016.

[20] Z. Zhang and Q. Yu, “Modeling Hardware Trojans in 3-D ICs,” *Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pp. 483–488, July 2019.

[21] I. Savidis and E. G. Friedman, “Electrical Modeling and Characterization of 3-D Vias,” *Proceedings of the IEEE International Symposium on Circuits and Systems*, pp. 784–787, May 2008.

[22] R. J. Masti, D. Rai, A. Ranganathan, C. Müller, L. Thiele, and S. Capkun, “Thermal Covert Channels on Multi-core Platforms,” *Proceedings of the USENIX Security Symposium (USENIX Security 15)*, August 2015.

[23] J. Knechtel and O. Sinanoglu, “On Mitigation of Side-channel Attacks in 3-D ICs: Decorrelating Thermal Patterns From Power and Activity,” *Proceedings of the ACM/IEEE Design Automation Conference (DAC)*, pp. 1–6, June 2017.

[24] P. Gu, D. Stow, R. Barnes, E. Kursun, and Y. Xie, “Thermal-aware 3-D Design for Side-channel Information Leakage,” *Proceedings of the IEEE International Conference on Computer Design (ICCD)*, pp. 520–527, October 2016.

[25] J. Dofe and Q. Yu, “Exploiting PDN Noise to Thwart Correlation Power Analysis Attacks in 3-D ICs,” *Proceedings of the ACM System Level Interconnect Prediction (SLIP) Workshop*, pp. 1–6, June 2018.

[26] Z. Zhang, “A Comprehensive Study of the Hardware Trojan and Side-Channel Attacks in Three-Dimensional (3-D) Integrated Circuits (ICs),” *Doctoral Dissertation 2642, University of New Hampshire*, October 2021.

[27] S. Picek, A. Heuser, A. Jovic, S. A. Ludwig, S. Guilley, D. Jakobovic, and N. Mentens, “Side-channel Analysis and Machine Learning: A Practical Perspective,” *Proceedings of the International Joint Conference on Neural Networks (IJCNN)*, pp. 4095–4102, May 2017.

[28] J. Benesty, J. Chen, Y. Huang, and I. Cohen, “Pearson Correlation Coefficient,” *Noise Reduction in Speech Processing, Springer Berlin Heidelber*, pp. 1–4, March 2009.

[29] E. Brier, C. Clavier, and F. Olivier, “Correlation Power Analysis with a Leakage Model,” *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, pp. 16–29, August 2004.

[30] J. Dofe, Chen Y., S. Kontak, E. Salman, and Q. Yu, “Transistor-level Camouflaged Logic Locking Method for Monolithic 3-D IC Security,” *Proceedings of the IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)*, pp. 1–6, December 2016.