3D Integration: Another Dimension Toward Hardware Security

Johann Knechtel, Satwik Patnaik, and Ozgur Sinanoglu
Tandon School of Engineering, New York University, New York, USA
Division of Engineering, New York University Abu Dhabi, United Arab Emirates
{johann, sp4012, ozgursin}@nyu.edu

***Abstract*—We review threats and selected schemes concerning hardware security at design and manufacturing time as well as at runtime. We find that 3D integration can serve well to enhance the resilience of different hardware security schemes, but it also requires thoughtful use of the options provided by the umbrella term of 3D integration. Toward enforcing security at runtime, we envision secure 2.5D system-level integration of untrusted chips and "all around" shielding for 3D ICs.**

***Index Terms*—Hardware Security, 3D Integration**

I. Introduction

Given the fact that integrated circuits (ICs) are at the heart of ubiquitous information technology, IC designers and vendors should seek to establish trust into their products by all available means. However, doing so is a practical challenge as related efforts deviate from the typically security-unaware design and manufacturing flows. For example, it has been shown that the speculative execution in processors, which is an industry-wide best practice, can be exploited to leak sensitive data [1]. Besides such concerns regarding data at runtime, the field of hardware security also spans other design- and manufacturing-time threats such as reverse engineering (RE), intellectual property (IP) piracy, overproduction, or insertion of hardware Trojans (HTs) [2]. The latter threats arise due to outsourcing, which is a predominant trend for IC supply chains, as it is the case for many other industries nowadays.

Aside from traditional 2D IC manufacturing, research and development for 3D integration has made significant progress over recent years. 3D integration means to stack and interconnect multiple chips or active layers. There are two main drivers for 3D integration [3], [4]: (1) the CMOS scalability bottleneck, which becomes more exacerbated for advanced nodes by issues like routability, pitch scaling, and process variations; and (2) the need to advance means for heterogeneous and system-level integration. Both drivers are also known as (1) "More Moore" and (2) "More than Moore." Various studies, prototypes, and commercial products have shown that 3D integration can indeed offer significant benefits over conventional 2D ICs, e.g., see [5], [6], [7], [8].

The umbrella term of 3D integration comprises four different flavors as follows (Fig. 1):

(a) Through-silicon via (TSV) 3D ICs, where multiple chips are fabricated separately and then stacked and bonded. The vertical interconnects across the 3D ICs are realized by relatively large metal TSVs which are cutting through the individual chips.

This work was supported in part by NYUAD under REF Grant RE218 and by NYU/NYUAD Center for Cybersecurity (CCS).

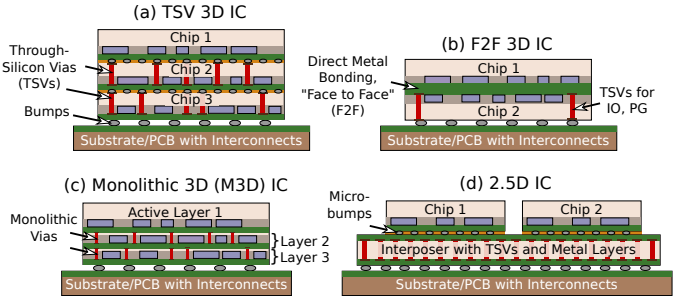

Fig. 1. Four flavors of 3D integration. Metal layers are colored in green, active layers in brown, along with logic in blue, and bonding layers in yellow.

(b) Face-to-face (F2F) 3D ICs, where two chips are fabricated separately and then bonded directly at their back-end-of-line (BEOL) metal "faces." TSVs or wirebonds are commonly used for external connections.

(c) Monolithic 3D (M3D) ICs, where multiple active layers are manufactured sequentially. The vertical interconnects are implemented by regular metal vias.

(d) 2.5D ICs, where chips are fabricated separately and then stacked and bonded onto a system-level interconnect carrier, the so-called interposer. This interposer can be either passive, comprising only metal layers and possibly some discrete devices, or active, containing some logic.

In this paper, we discuss prior art concerning hardware security in general. We then elaborate how 3D integration offers unique opportunities to advance such schemes, along with a review of recent studies.

II. Protection of Design IP

Independent of 2D IC manufacturing or modern 3D integration, various techniques have been proposed over the years toward protection of chip design IP. Most works fall under one of the following three categories: logic locking (LL), layout camouflaging (LC), or split manufacturing (SM). All three schemes consider different threats; LL is concerned about untrusted end-users and malicious foundries, SM about untrusted foundries, and LC about untrusted end-users. The interested reader may also want to see [9] for more details.

Now, 3D integration can serve to advance these schemes in different ways. The main benefit provided by 3D integration is the *physical separation* of components, as dictated by the security-enforcing designer and/or vendor, be it across interconnects, active devices, or both. In Table I, we provide an overview on selected works, which are also discussed next.

© 2019 IEEE. This is the author's version of the work. It is posted here for your personal use. Not for redistribution.
The definitive Version of Record is published in Proc. IEEE Int. On-Line Test Symp. (IOLTS), 2019.

TABLE I
SELECTED 3D SCHEMES TARGETING AT MANUFACTURING TIME

Reference	Style	Scheme	Scope	Assets	Trusted Facility
[10]	2.5D	SM	IP Piracy	Wires	BEOL
[11]	2.5D	SM	HT Prevent.	Wires	BEOL
[12]	F2F	SM & LC	IP Piracy	Gates & Wires	FEOL & BEOL
[13]	M3D	LC	IP Piracy	Gates	FEOL
[14]	F2F	SM & LC	IP Piracy	Gates & Wires	BEOL

A. Logic Locking

To the best of our knowledge, 3D integration has not been explored yet for LL. In a loosely related work by Sengupta *et al.* [15], the authors leverage formal principles pertaining to LL in order to advance the notion of SM. More specifically, they lock the FEOL and delegate the unlocking to a separate, trusted BEOL facility, namely by implementing the LL key via BEOL-level routing toward fixed-logic drivers. The authors note that their scheme can also be realized at the package or board level, which suggests an implementation as 2.5D IC.

B. Camouflaging

Yan *et al.* [13] were first to propose LC dedicated for 3D integration, more specifically for monolithic 3D ICs. The authors developed and characterized custom libraries, and they evaluated their scheme at both the cell and the chip scale. The device-level camouflaging is realized by dummy contacts, which has been proposed already previously for LC in classical 2D ICs. Thus, while conceptionally not new, the work in [13] leverages the benefits provided by monolithic 3D ICs, in an effort to advance the scalability of LC. That is noteworthy because prior art for 2D-centric LC may incur excessive PPA cost. For example, the 2D NAND-NOR-XOR primitive of [16] would incur 5.5× power, 1.6× delay, and 4× area cost compared to a regular NAND gate.[1] In contrast, Yan *et al.* [13] report on average 25% power cost, 15% delay cost, and 43% area *savings* compared to regular 2D gates.

C. Split Manufacturing

As indicated by the terminology, SM means to split the manufacturing flow, typically into an untrusted FEOL process and a trusted BEOL process thereafter. For the FEOL facility, a split layout appears like a "sea of gates," making it difficult to infer the complete netlist readily. Still, since physical-design tools work holistically on both FEOL and BEOL, various traces can well remain in the FEOL [19], [20].

To advance SM, leveraging 3D integration is straightforward and also promising. That is because 3D integration allows to split a design into multiple chips, which can maintain their FEOL and BEOL layers independently, whereas the 2.5D/3D stack can comprise further parts of the system-level interconnects. This system-level nature of 3D SM allows to manufacture, test, and withhold various functional components from untrusted parties, all as need be. Moreover, concerns regarding the practicability of classical 2D SM can be elevated due to this very fact that the 2.5D/3D stack can hold additional system-level interconnects independently of the regular FEOL and BEOL processing of individual chips.

[1]The excessive cost of 2D LC schemes would arguably allow only for few gates being camouflaged. This, in turn, renders prior art either fully prone to analytical attacks, e.g., see the Boolean satisfiability (SAT) framework in [17], or it calls for advanced, SAT-resilient schemes. By nature, however, such schemes are low-corruptibility ones, thereby enabling an attacker to obtain at least an approximate version of the IP [18].

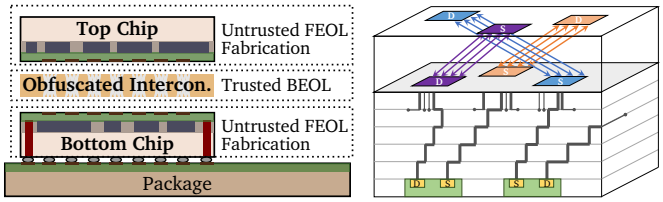

Fig. 2. Key concepts for 3D split manufacturing with camouflaging, as proposed in [14]. (a) Obfuscated interconnects are added to render RE more difficult. (b) Randomized routing to hinder FEOL-foundry-based adversaries from inferring the netlist. For simplicity, only the bottom chip and the additional, trusted BEOL interconnects are indicated.

The idea of 3D SM was outlined already in 2008, by Tezzaron Semiconductor Corp. [21]. Various early studies were hinting at 3D SM as well, but most had some limitations. For example, Dofe *et al.* [22] remained on the conceptional level. Xie *et al.* [10] and Imeson *et al.* [11] utilized 2.5D integration with "only" wires being hidden from untrusted facilities—in principle, this is equivalent to traditional SM for 2D ICs but, as indicated, it is more practical. Still, the studies [10], [11] suffer from considerable layout cost.

Later on, DeVale *et al.* [23], Gu *et al.* [12], and Patnaik *et al.* [14] explored SM in the context of 3D ICs, effectively promoting "native 3D SM." One key findings of those later studies is that both the partitioning as well as the design of the vertical interconnects play an important role and define a cost-security trade-off as follows. The more the design is split across multiple chips, the higher the layout cost can become (also due to the need for more vertical interconnects), but the more flexibility an security-enforcing designer has to separate components and thereby "dissolve" the IP across the 3D stack.

D. Split Manufacturing and Camouflaging in Conjunction

Both Gu *et al.* [12] and Patnaik *et al.* [14] proposed 3D SM in conjunction with LC. While Gu *et al.* [12] consider regular, FEOL-centric LC, Patnaik *et al.* [14] argue that another approach is more appropriate, namely the obfuscation of the vertical interconnects.

In their work [14], the authors propose to include additional metal layers as redistribution layers (RDLs) between the chips of an F2F 3D IC. As illustrated in Fig. 2, these additional layers comprise (a) obfuscated interconnects (without loss of generality using magnesium- and magnesium-oxide-based vias) to render RE of the 3D IC more difficult, and (b) randomized routing paths such that regular stacking of the chips will not readily reveal these missing interconnects. By doing so, their work addresses both malicious foundries and end-users, along with affordable layout and manufacturing cost [14].

Besides LC along with 3D SM as outlined above, other works suggest camouflaging at the system level. More specifically, Dofe *et al.* [24] propose to obfuscate the vertical communication links in 3D ICs by rerouting within dedicated network-on-chip structures (NoCs) "sandwiched" between the chips. In that sense, their idea is similar but more flexible to

© 2019 IEEE. This is the author's version of the work. It is posted here for your personal use. Not for redistribution.
The definitive Version of Record is published in Proc. IEEE Int. On-Line Test Symp. (IOLTS), 2019.

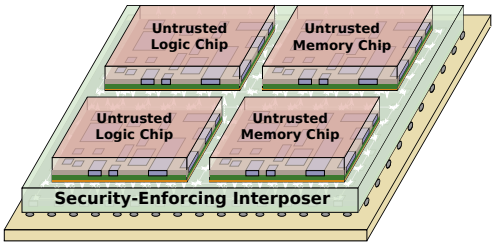

Fig. 3. Our concept for a secure 2.5D system-level integration of untrusted chips. All communication between chips and memories are monitored by the security features residing in the active, security-enforcing interposer.

the randomized routing outlined above for Patnaik *et al.* [14], although it is also more costly as it requires dedicated active layers instead of only metal layers.

III. Hardware Security at Runtime

Aside from the need for protecting the design IP and rendering the globalized supply chain more trustworthy, there are also various security risks arising at runtime. The major threats are (i) unauthorized access or modification of data and (ii) invasive probing or modification of the hardware or its behavior. For (i), this can occur via malicious software, HTs, side-channel attacks, misuse of test infrastructures, etc. For (ii), this comprises scenarios like focused-ion beam milling, monitoring of photon emission, fault injection, etc.

Similar to the case of IP protection, 3D integration can also advance schemes focused on security at runtime, again by the virtue of physical separation. Next, we provide an overview on selected works, and we also propose some novel concepts.

A. Monitoring or Verification of Untrusted ICs

In general, various monitoring or verification schemes have been proposed toward continuous control of ICs, e.g., see [25], [26], [27], [28]. The common objective of these works is to detect any malicious or unexpected behaviour at runtime, emanating from software, hardware, or even both.

Extending such schemes via 3D integration is particularly promising. That is because the security-critical components can be implemented separately using a trusted fabrication process and 3D-integrated later on with the commodity chip to be monitored [28], [29], [30]. Still, we caution that the physical implementation can become a vulnerability by itself. In [30], for example, the authors propose "introspective interfaces" which, however, require additional logic within the commodity chip to be monitored. It is easy to see that these interfaces could fail when they are modified by any malicious actor involved with the design or manufacturing of that commodity chip. Thus, a undesirable dependency arises, possibly thwarting the scheme altogether. We note that the authors themselves acknowledge this limitation for their work in [30].

Here we envision an alternative for secure monitoring at runtime, based on 2.5D integration (Fig. 3). The essence of our approach is to provide a proper, system-level separation of untrusted commodity and trusted security components. That is, all the physical interfaces and security features are delegated exclusively to an active interposer, which also serves as system-level interconnect backbone and integration carrier. Active interposer have been successful demonstrated, e.g., see [31]; they can also be implemented using an old but trusted facility, thereby possibly allowing for cost savings.

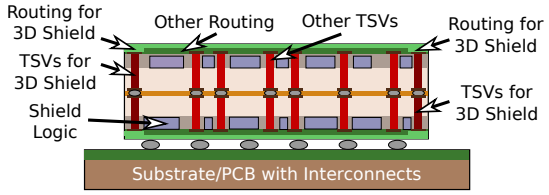

Fig. 4. Our proposal for "all around" shielding in 3D ICs. The most suitable integration style is back-to-back (B2B) stacking, since it allows to protect the substrate backsides from invasive probing and non-invasive readout attacks. The frontsides comprise dedicated layers/routing paths for the shield (light green), which are complemented by shield TSVs (dark red) placed at the IC boundaries. The shield logic is integrated along with regular logic.

B. Probing, Monitoring, or Circuit Modification Attacks

Semi- or fully-invasive probing, monitoring, fault injection, or even circuit modifications are arguably the most severe threats for hardware security at runtime. Related attacks and various countermeasures have been demonstrated for classical 2D ICs, e.g., see [32], [33], [34] and [35], [36], [37], [38].

Despite the severity of those threats on the one hand, we also emphasize that, on the other hand, the benefits which 3D integration can offer to protect against such threats are outstanding. To the best of our knowledge, 3D integration is the only enabler for an "all around" shield approach. That is, only within 3D ICs we can build up a fully enveloping 3D shield structure (Fig. 4). Such a 3D shield would comprise (i) dedicated metal layers/wires building up individual shields for both the chips, and (ii) TSVs to interconnect the shields of the two chips. Toward the logical and physical design of the individual shields, prior art can be leveraged readily, e.g., see [36], [38]. Besides hindering probing attacks, we believe that such a 3D shield could also hinder other non-invasive but powerful attacks, e.g., monitoring of the photon emission [33].

Similar protection has been discussed before in [35], [36]. However, the true potential for 3D shields has not been explored yet; the authors of those early studies considered techniques like B2B stacking either as out-of-scope or as impractical, although without providing any substantiated critic.

C. Side-Channel Attacks and Hardware Trojans

Conducting a side-channel attack (SCA) means to carefully examine the physical emanations of an IC under attack, in order to extract some sensitive information. SCAs are powerful and hard to prevent since any electronic device is inevitably subject to physical side-channels emissions at runtime. For example, it has been shown that the timing of caches or power consumption can be exploited to infer secret keys [39].

On the one hand, prior art considers SCAs which are targeted explicitly for 3D ICs. For example, Gu *et al.* [40] and Knechtel and Sinanoglu [41] seek to hinder thermal SCAs on 3D ICs at runtime and design time, respectively, whereas Dofe *et al.* [42] seek to hinder power SCAs on 3D ICs. On the other hand, some studies leverage the benefits provided by 3D integration to apply security techniques otherwise considered too costly. For example, Bao and Srivastava [43] impose random eviction and differing latencies across a cache

© 2019 IEEE. This is the author's version of the work. It is posted here for your personal use. Not for redistribution.
The definitive Version of Record is published in Proc. IEEE Int. On-Line Test Symp. (IOLTS), 2019.

architecture. The authors show that such techniques incur high performance cost in classical 2D ICs but can be realized even with some performance gains in a 3D IC.

Mossa *et al.* [44] have cautioned that HTs can become more stealthy and effectively tailored for 3D ICs than for 2D ICs. The authors explore thermal triggers in detail, motivated by the fact that thermal management is a well-known challenge for 3D ICs by itself. Finally, in a similar but general manner, we like to caution that the broader landscape of suppliers and actors involved with 3D integration can open up new opportunities for attackers to embed different types of HTs.

IV. Summary

In this short paper, we have reviewed major threats and selected schemes concerning hardware security at design/manufacturing time as well as at runtime. We note that 3D integration serves well to enhance different approaches for hardware security, but it also requires careful use of those novel 3D techniques. We have also outlined two advanced schemes for enforcing security at runtime, one based on 2.5D system-level integration of untrusted commodity chips, and one based on "all around" 3D shielding.

References

[1] P. Kocher *et al.*, "Spectre attacks: Exploiting speculative execution," *Proc. Symp. Sec. Priv.*, vol. 1, pp. 19–37, 2019.

[2] S. Bhunia, S. Ray, and S. Sur-Kolay, Eds., *Fundamentals of IP and SoC Security*. Springer, 2017.

[3] J. Knechtel and J. Lienig, "Physical design automation for 3D chip stacks – challenges and solutions," in *Proc. Int. Symp. Phys. Des.*, 2016, pp. 3–10, invited paper.

[4] J. Knechtel *et al.*, "Large-scale 3D chips: Challenges and solutions for design automation, testing, and trustworthy integration," *Trans. Sys. LSI Des. Method.*, vol. 10, pp. 45–62, 2017, invited paper.

[5] D. Fick *et al.*, "Centip3De: A cluster-based NTC architecture with 64 ARM Cortex-M3 cores in 3D stacked 130 nm CMOS," *J. Sol.-St. Circ.*, vol. 48, no. 1, pp. 104–117, 2013.

[6] S. S. Iyer, "Three-dimensional integration: An industry perspective," *MRS Bulletin*, vol. 40, no. 3, pp. 225–232, 2015.

[7] D. H. Kim *et al.*, "3D-MAPS: 3D massively parallel processor with stacked memory," in *Proc. Int. Sol.-St. Circ. Conf.*, 2012, pp. 188–190.

[8] A. Shilov. (2018) AMD previews EPYC Rome processor: Up to 64 Zen 2 cores. [Online]. Available: https://www.anandtech.com/show/13561/amd-previews-epyc-rome-processor-up-to-64-zen-2-cores

[9] J. Knechtel, S. Patnaik, and O. Sinanoglu, "Protect your chip design intellectual property: An overview," in *Proc. Conf. Omni-Layer Intell. Sys.*, 2019, pp. 211–216, invited paper.

[10] Y. Xie, C. Bao, and A. Srivastava, "Security-aware 2.5D integrated circuit design flow against hardware IP piracy," *Computer*, vol. 50, no. 5, pp. 62–71, 2017.

[11] F. Imeson, A. Emtenan, S. Garg, and M. V. Tripunitara, "Securing computer hardware using 3D integrated circuit (IC) technology and split manufacturing for obfuscation," in *Proc. USENIX Sec. Symp.*, 2013, pp. 495–510.

[12] P. Gu *et al.*, "Cost-efficient 3D integration to hinder reverse engineering during and after manufacturing," in *Proc. Asian Hardw.-Orient. Sec. Trust Symp.*, 2018, pp. 74–79.

[13] C. Yan *et al.*, "Hardware-efficient logic camouflaging for monolithic 3D ICs," *Trans. Circ. Sys.*, vol. 65, no. 6, pp. 799–803, 2018.

[14] S. Patnaik, M. Ashraf, O. Sinanoglu, and J. Knechtel, "Best of both worlds: Integration of split manufacturing and camouflaging into a security-driven CAD flow for 3D ICs," in *Proc. Int. Conf. Comp.-Aided Des.*, 2018, pp. 8:1–8:8.

[15] A. Sengupta, M. Nabeel, J. Knechtel, and O. Sinanoglu, "A new paradigm in split manufacturing: Lock the FEOL, unlock at the BEOL," in *Proc. Des. Autom. Test Europe*, 2019, pp. 414–419.

[16] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security analysis of integrated circuit camouflaging," in *Proc. Comp. Comm. Sec.*, 2013, pp. 709–720.

[17] C. Yu *et al.*, "Incremental SAT-based reverse engineering of camouflaged logic circuits," *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, vol. 36, no. 10, pp. 1647–1659, 2017.

[18] K. Shamsi *et al.*, "AppSAT: Approximately deobfuscating integrated circuits," in *Proc. Int. Symp. Hardw.-Orient. Sec. Trust*, 2017, pp. 95–100.

[19] Y. Wang, P. Chen, J. Hu, and J. J. Rajendran, "The cat and mouse in split manufacturing," in *Proc. Des. Autom. Conf.*, 2016, pp. 165:1–165:6.

[20] H. Li *et al.*, "Attacking split manufacturing from a deep learning perspective," in *Proc. Des. Autom. Conf.*, 2019, pp. 135:1–135:6.

[21] "3D-ICs and integrated circuit security," Tezzaron Semiconductor, 2008. [Online]. Available: http://tezzaron.com/media/3D-ICs_and_Integrated_Circuit_Security.pdf

[22] J. Dofe *et al.*, "Security threats and countermeasures in three-dimensional integrated circuits," in *Proc. Great Lakes Symp. VLSI*, 2017, pp. 321–326.

[23] J. DeVale, R. Rakvic, and K. Rudd, "Another dimension in integrated circuit trust," *J. Cryptogr. Eng.*, vol. 8, no. 4, pp. 315–326, 2017.

[24] J. Dofe, Q. Yu, H. Wang, and E. Salman, "Hardware security threats and potential countermeasures in emerging 3D ICs," in *Proc. Great Lakes Symp. VLSI*, 2016, pp. 69–74.

[25] L. W. Kim and J. D. Villasenor, "A system-on-chip bus architecture for thwarting integrated circuit trojan horses," *Trans. VLSI Syst.*, vol. 19, no. 10, pp. 1921–1926, 2011.

[26] S. Bhunia *et al.*, "Protection against hardware trojan attacks: Towards a comprehensive solution," *Des. Test*, vol. 30, no. 3, pp. 6–17, 2013.

[27] A. Chandrasekharan, K. Schmitz, U. Kuhne, and R. Drechsler, "Ensuring safety and reliability of IP-based system design – a container approach," in *Proc. Int. Symp. Rapid System Prototyping*, 2015, pp. 76–82.

[28] R. S. Wahby, M. Howald, S. Garg, and M. Walfish, "Verifiable ASICs," *Proc. Symp. Sec. Priv.*, pp. 759–778, 2016.

[29] S. Mysore *et al.*, "Introspective 3D chips," *SIGOPS Operat. Sys. Rev.*, vol. 40, no. 5, pp. 264–273, 2006.

[30] J. Valamehr *et al.*, "A 3-D split manufacturing approach to trustworthy system development," *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, vol. 32, no. 4, pp. 611–615, 2013.

[31] F. Clermidy *et al.*, "New perspectives for multicore architectures using advanced technologies," in *Proc. Int. Elec. Devices Meeting*, 2016, pp. 35.1.1–35.1.4.

[32] C. Helfmeier *et al.*, "Breaking and entering through the silicon," in *Proc. Comp. Comm. Sec.*, 2013, pp. 733–744.

[33] S. Tajik, H. Lohrke, J.-P. Seifert, and C. Boit, "On the power of optical contactless probing: Attacking bitstream encryption of FPGAs," in *Proc. Comp. Comm. Sec.*, 2017, pp. 1661–1674.

[34] H. Wang, Q. Shi, D. Forte, and M. M. Tehranipoor, "Probing attacks on integrated circuits: Challenges and research opportunities," *Des. Test*, vol. 34, no. 5, pp. 63–71, 2017.

[35] S. Briais *et al.*, "3D hardware canaries," in *Proc. Cryptogr. Hardw. Embed. Sys.*, 2012, pp. 1–22.

[36] J. M. Cioranesco *et al.*, "Cryptographically secure shields," in *Proc. Int. Symp. Hardw.-Orient. Sec. Trust*, 2014, pp. 25–31.

[37] K. Yi, M. Park, and S. Kim, "Practical silicon-surface-protection method using metal layer," *J. Semicond. Tech. Sci.*, vol. 16, no. 4, pp. 470–480, 2016.

[38] M. Weiner, S. Manich, R. Rodríguez-Montañés, and G. Sigl, "The low area probing detector as a countermeasure against invasive attacks," *Trans. VLSI Syst.*, vol. 26, no. 2, pp. 392–403, 2018.

[39] Y. Zhou and D. Feng, "Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing," in *IACR Crypt. ePrint Arch.*, no. 388, 2005.

[40] P. Gu *et al.*, "Thermal-aware 3D design for side-channel information leakage," in *Proc. Int. Conf. Comp. Des.*, 2016, pp. 520–527.

[41] J. Knechtel and O. Sinanoglu, "On mitigation of side-channel attacks in 3D ICs: Decorrelating thermal patterns from power and activity," in *Proc. Des. Autom. Conf.*, 2017, pp. 12:1–12:6.

[42] J. Dofe *et al.*, "Impact of power distribution network on power analysis attacks in three-dimensional integrated circuits," in *Proc. Great Lakes Symp. VLSI*, 2017, pp. 327–332.

[43] C. Bao and A. Srivastava, "3D integration: New opportunities in defense against cache-timing side-channel attacks," in *Proc. Int. Conf. Comp. Des.*, 2015, pp. 273–280.

[44] S. F. Mossa, S. R. Hasan, and O. Elkeelany, "Self-triggering hardware trojan: Due to NBTI related aging in 3-D ICs," *Integration*, vol. 58, no. Supplement C, pp. 116–124, 2017.

© 2019 IEEE. This is the author's version of the work. It is posted here for your personal use. Not for redistribution. The definitive Version of Record is published in Proc. IEEE Int. On-Line Test Symp. (IOLTS), 2019.