IPSJ Transactions on System LSI Design Methodology Vol.10 45–62 (Aug. 2017)

[DOI: 10.2197/ipsjtsldm.10.45]

Invited Paper

Large-Scale 3D Chips: Challenges and Solutions for Design Automation, Testing, and Trustworthy Integration

Johann Knechtel[1,a) Ozgur Sinanoglu[1,b) Ibrahim (Abe) M. Elfadel[2,c) Jens Lienig[3,d)
Cliff C. N. Sze[4,e)

Received: March 1, 2017

Abstract: Three-dimensional (3D) integration of electronic chips has been advocated by both industry and academia for many years. It is acknowledged as one of the most promising approaches to meet ever-increasing demands on performance, functionality, and power consumption. Furthermore, 3D integration has been shown to be most effective and efficient once large-scale integration is targeted for. However, a multitude of challenges has thus far obstructed the mainstream transition from "classical 2D chips" to such large-scale 3D chips. In this paper, we survey all popular 3D integration options available and advocate that using an *interposer* as system-level integration backbone would be the most practical for large-scale industrial applications and design reuse. We review major design (automation) challenges and related promising solutions for interposer-based 3D chips in particular, among the other 3D options. Thereby we outline (*i*) the need for a unified workflow, especially once full-custom design is considered, (*ii*) the current design-automation solutions and future prospects for both classical (digital) and advanced (heterogeneous) interposer stacks, (*iii*) the state-of-art and open challenges for testing of 3D chips, and (*iv*) the challenges of securing hardware in general and the prospects for large-scale and trustworthy 3D chips in particular.

Keywords: 3D chips, large-scale integration, system-level integration, heterogeneous integration, design automation, testing, hardware security, trustworthy integration

1. Introduction

3D chips—multiple vertically (and/or laterally) stacked and interconnected layers of active components (and/or whole chips)—are often claimed to meet current and future requirements for electronic devices. By their stacked and densely integrated nature, 3D chips offer shorter interconnects and, thus, reduced delays and power, and increased performance [1], [2], [3]. At the same time, both digital and heterogeneous components spread across multiple chips/dies are relatively easy to integrate into one common 3D stack. Note that such heterogeneous 3D chips, if tailored for small footprints and low power consumption, are also essential for widely-anticipated applications such as the Internet of Things (IoT). Two prominent design paradigms, namely "More Moore" (shrinking device nodes and leveraging new materials) and "More-than-Moore" (heterogeneous integration), advocate both for 3D chips in particular [4] (**Fig. 1**).

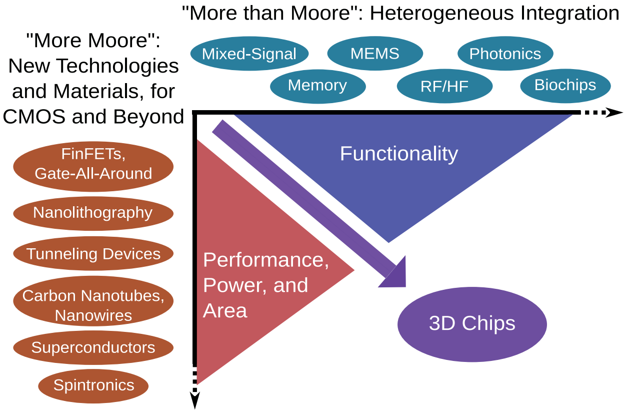

"More than Moore": Heterogeneous Integration
"More Moore": New Technologies and Materials, for CMOS and Beyond
Mixed-Signal
MEMS
Photonics
Memory
RF/HF
Biochips
FinFETs, Gate-All-Around
Nanolithography
Tunneling Devices
Carbon Nanotubes, Nanowires
Superconductors
Spintronics
Functionality
Performance, Power, and Area
3D Chips

Fig. 1 The well-known "More Moore" trend for down-scaling the nodes is slowly but surely reaching its limits for CMOS technology. New technologies and materials are being investigated, but most are not mature yet for high-volume manufacturing. "More than Moore", which targets for heterogeneous integration, has been identified as another important direction. The concept of 3D chips offers the potential to meet both trends at the same time.

Despite the significant benefits projected over 2D chips in general, and the recent high-volume emergence of 3D memory stacks (such as *High-Bandwidth Memory, HBM* [5], [6]) in particular, the overall adoption of 3D chips still lags behind expectations—academic and industry leaders have been promoting 3D integration for more than one decade now [1], [2], [7], [8]. Successful adoption of 3D chips requires addressing different classical and novel challenges which simultaneously affect the manufacturing processes, design practices and physical design tools [3], [9], [10], [11], [12], [13]. If not properly addressed, these fairly complex challenges (such as adverse coupling effects [14], [15]) may render 3D chips commercially unviable.

[1] New York University Abu Dhabi, PO Box 129188, Abu Dhabi, UAE
[2] Masdar Institute, Khalifa University of Science and Technology, PO Box 54224, Abu Dhabi, UAE
[3] TU Dresden, 01062 Dresden, Germany
[4] Google Inc., Austin, Texas 78705, USA
[a)] johann@nyu.edu
[b)] ozgursin@nyu.edu
[c)] ielfadel@masdar.ac.ae
[d)] jens.lienig@tu-dresden.de
[e)] csze@google.com

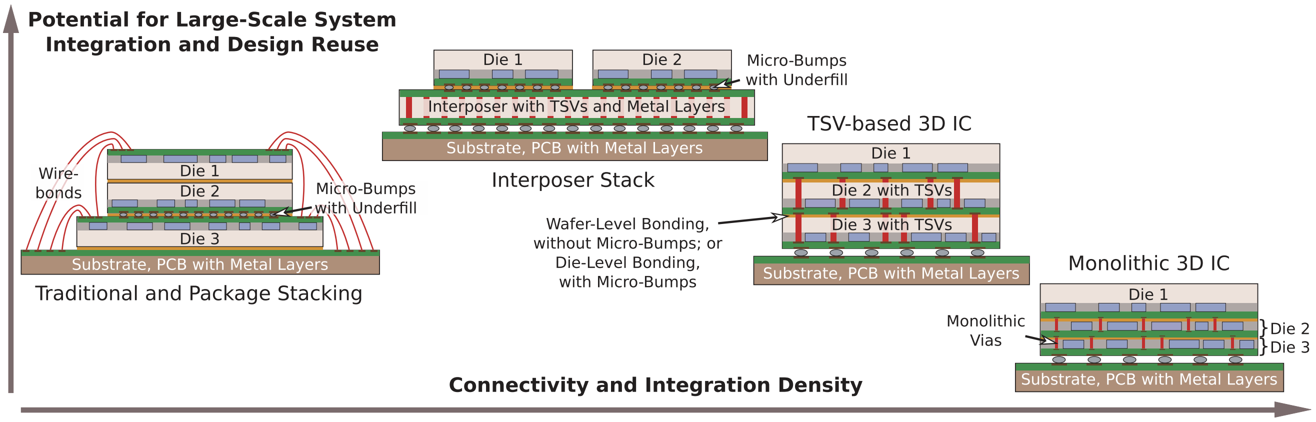

Potential for Large-Scale System Integration and Design Reuse
Wire-bonds
Die 1
Die 2
Die 3
Micro-Bumps with Underfill
Substrate, PCB with Metal Layers
Traditional and Package Stacking
Die 1
Die 2
Micro-Bumps with Underfill
Interposer with TSVs and Metal Layers
Substrate, PCB with Metal Layers
Interposer Stack
TSV-based 3D IC
Die 1
Die 2 with TSVs
Die 3 with TSVs
Wafer-Level Bonding, without Micro-Bumps; or Die-Level Bonding, with Micro-Bumps
Substrate, PCB with Metal Layers
Monolithic 3D IC
Die 1
Monolithic Vias
Die 2
Die 3
Substrate, PCB with Metal Layers
Connectivity and Integration Density

Fig. 2 Implementation options for 3D chips. Originating with traditional and package stacking using mainly flip-chip and wire bonding, 3D integration has evolved towards interposer stacks (also known as “2.5D integration”) as well as towards more encapsulated options: through silicon-via (TSV)-based 3D ICs and monolithic 3D ICs. While the latter two options provide the highest integration densities and connectivity, the other options, especially modern interposer stacks, facilitate large-scale, system-level integration and chip-level design reuse.

Physical design automation, among other stages such as testing, partially meets these challenges already at present, but further efforts are needed to exploit the full potential of 3D chips and to facilitate their wide-scale commercial breakthrough.

In this paper, we elaborate on these challenges and review promising solutions. A key observation is that most challenges can be eased once system-level 3D integration (of 2D chips) is pursued. The related concept of *interposer-based 3D integration* is widely accepted nowadays [8], [16], [17], [18], [19], [20], [21], [22]; it is a practical, flexible, and cost-effective alternative to the previously more anticipated full-custom and native 3D integration.

Here we initially provide an overview on 3D integration in general and its design-automation challenges in particular (in the remainder of this Section 1). In Sections 2 and 3, we then discuss the respective challenges and solutions for design automation of interposer in general and heterogeneous interposer in particular. In Section 4, we review the state-of-art for testing of 3D chips and we outline open challenges. In Section 5, we address hardware security, an important aspect for modern chip design, especially for advanced and complex devices such as 3D chips. Finally, we summarize and conclude in Section 6.

1.1 Implementation Options for 3D Chips

3D chips can be classified into four categories (**Fig. 2**): (*i*) traditional and package stacking, (*ii*) interposer stacks, (*iii*) through-silicon via (TSV)-based 3D ICs, and (*iv*) monolithic 3D ICs. Note that advanced 3D stacks may cross different categories, such as when multiple TSV-based 3D ICs are integrated on an interposer.

Each option has its scope of application, with distinctive benefits and drawbacks, as well as requirements for design and manufacturing processes. On the one end of the scale, monolithic 3D ICs enable the highest integration density (i.e., transistor-level 3D integration), but this requires full-custom design and dedicated manufacturing steps, which both hinders system-level integration and design reuse. On the other end of the scale, interposer stacks as well as traditional and package stacking (originated with flip-chip and wire bonding) allow for reuse of legacy 2D chips, but only with limited integration and interconnectivity rates.

In the following, key aspects of the 3D implementation options are reviewed and design challenges are outlined. Further technical details have been reviewed, e.g., by *imec*’s Eric Beyne in Ref. [23], here along with the related 2D and 3D interconnect topologies.

Traditional and package stacking has been widely adopted in the past; it is thus not reviewed in detail in our paper*1.

1.1.1 TSV-based 3D ICs

This option has initially attracted the most attention and research and development efforts; many prototypes and products nowadays are based on TSV technology [2], [5], [6], [18], [28], [29], [30], [31]. The key element, the through-silicon vias (TSVs) are metal plugs (typically copper or tungsten) that penetrate whole stacked dies in order to interconnect those dies. Different options for stacking of the dies are applicable [23], [32]; for example, *face-to-back* stacking is where the metal layers (the “face”) of one die are bonded to the substrate (the “back”) of another die.

Depending on the TSV process (**Fig. 3**), different design challenges arise: *via-first TSVs* and *via-middle TSVs* obstruct the device layer and result in placement obstacles; *via-last TSVs* obstruct the device layer and the metal layers, resulting in placement and routing obstacles. Due to their relatively large diameter and intrusive character, TSVs can neither be deployed excessively nor arbitrarily; they have to be optimized in count and arrange-

*1 Even though they are not strictly stacking-centric, there are modern packaging approaches still worth mentioning for large-scale integration. One such approach is *fan-out-wafer-level packaging* (*FOWLP*) [12], and it is currently widely applied, e.g., in *Apple’s iPhone 7* [24], for its higher integration level and a greater number of external contacts than traditional wafer-level packaging. Another approach is that of the *embedded multi-die interconnect bridge* (*EMIB*) [25], [26]. Here a small chip slice with metal layers, called “bridge”, is embedded into the package substrate such that dies bonded above can be interconnected through it. Similarly as an interposer, an EMIB enables chip-level and high-bandwidth interconnectivity. An EMIB is less costly than an interposer, but it cannot offer a system-level integration platform like an interposer. The *Stratix 10 FPGA* [27] is a prominent high-end package using multiple EMIBs.

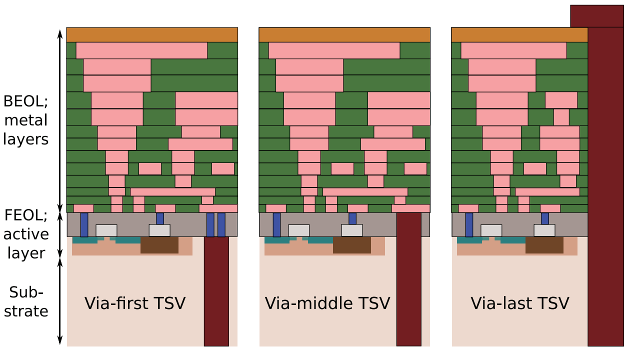


Fig. 3 The different TSV processes; illustration derived from Ref. [38]. Via-first TSVs are fabricated before the active layers (front-end-of-line, FEOL). Via-middle TSVs are fabricated after the FEOL but before the metal layers (back-end-of-line, BEOL). Via-last TSVs are fabricated after (or during) the BEOL process. According to Eric Beyne [23], via-middle TSVs are the most popular option for advanced 3D ICs as well as for interposer stacks.

ment [3], [13], [33], [34], [35], [36]. Note that TSVs do not scale at the same rate as transistors, thus the mismatch between TSV and cell dimensions will remain for future nodes and may even increase [37].

Overall, TSV-based 3D ICs enable chip-level integration of both homogeneous and heterogeneous dies but still require dedicated design and manufacturing steps. This limits their scope for large-scale and system-level design reuse. Besides, the integration density of TSV-based 3D ICs is lower than that of monolithic 3D ICs (but higher than that of interposer stacks).

1.1.2 Monolithic 3D ICs

This option has recently gained more attention [39], [40], [41], mainly thanks to advances of the processing technology [42]. The key feature of monolithic 3D ICs is that active layers are sequentially manufactured into one chip rather than bonded using separate dies. Due to their small vias, comparable to regular metal-stack vias, monolithic 3D ICs are the only option to enable fine-grained transistor-level integration. This is especially sought after for high-density and full-custom logic integration [39].

As for design challenges, both signal and power routing become notably more complex due to high congestion [39], [43]. However, once the area gain inherent in monolithic 3D ICs is traded-off, routability can become even significantly better than it is in 2D chips [41]. Besides, thermal properties differ from "classical" TSV-based 3D ICs: on the one hand, the regular vias are by far not as effective as TSVs for conducting heat out of the stack [44], [45]; on the other hand, monolithic chips do not exhibit potential "thermal barriers" in the form of bonding layers[*2]. Hence, the thermal coupling within monolithic stacks is larger and more uniform than for TSV-based 3D ICs, which calls for dedicated thermal management [45].

For placement, routing, and design closure of monolithic 3D ICs, the reuse of commercial 2D physical design tools has been demonstrated to lower the barrier for industry-wide acceptance [40], [47], [48], [49]. Nevertheless, due to its sequential processing nature, such 3D ICs cannot apply "plug-and-play" integration and large-scale design reuse as it is possible with the other 3D options.

1.1.3 Interposer Stacks

Interposer stacks are a widely accepted, cost-efficient alternative to 3D ICs [8], [16], [17], [18], [19], [20], [21], [22]. Here, active dies are arranged in lateral direction on a substrate—possibly on both of its sides—instead of stacking them strictly vertically. The interconnects are realized via TSVs and metal layers within the interposer (see Fig. 2).

Interposer stacks enable a heterogeneous design where chips/dies encompassing different technologies, e.g., "biochips," sensors, MEMS, and memory units, can be relatively easily connected in one package. As for homogeneous digital integration, interposer enable the partitioning of a large monolithic die (with low yield) into smaller dies (with higher yield) [19], [22]. This greatly lowers the overall manufacturing cost and also helps to improve the power efficiency. Further, interposer allow for better heat dissipation [17], [50]. In short, interposer are considered as the platform for "new multi-chip modules (MCMs)" [51], [52], with low cost, high yield, and the combination of heterogeneous integrated circuits in one package cited as the major advantages.

There exists a wide variety of interposer-based systems which can be categorized in different ways:

- According to the core material: silicon (today), organic (currently considered), or glass substrates (future) [16], [52], [53]
- According to the interposer type: fully passive, with embedded components such as microfluidic channels [54], or with active components [8], [20], [21], [55]
- According to the mounting approach: one-sided or double-sided die placement, distributed high-power or low-power die allocation [8]
- According to the chip design: prefabricated dies stacked onto the interposer (such as the *AMD Fiji/Fury* GPU with stacked HBM chips [56], [57], [58]) or custom dies designed for specific applications (such as the *Xilinx Virtex-7 FPGA* [59])

As of today, there are several products with interposer technology available on market, notably the *AMD Fiji/Fury GPU* [56], [57], [58] and the *Xilinx Virtex-7 FPGA* [59]. In 2016, *CEA Leti* demonstrated their second generation 3D-NoC technology [20], [21], which combines a series of small dies ("chiplets") fabricated at the FDSOI 28 nm node and co-integrated on a 65 nm CMOS interposer. The active interposer embeds several lower-cost functions, such as communication through the NoC and system I/Os, power conversion, design-for-testability, and integrated passive components. These products are all good examples leading to our belief that interposer stacks stand at the right spot in terms of the production-scale economy for 3D integration.

The design of interposer stacks is still manual to some degree; there is a lack of dedicated and advanced design tools [60]. Routing of active interposer and the related design of a large-scale network-on-chip (NoC), for example, requires further research efforts [61]. Other challenges such as simulation and verification of signal integrity across an interposer stack have been recently addressed [62], but require further efforts regarding tool integra-

[*2] For example, the micro-bump bonding in TSV-based 3D ICs may be underfilled with BCB polymer layers. This polymer has an approximately 600 times higher thermal resistivity than silicon [46].

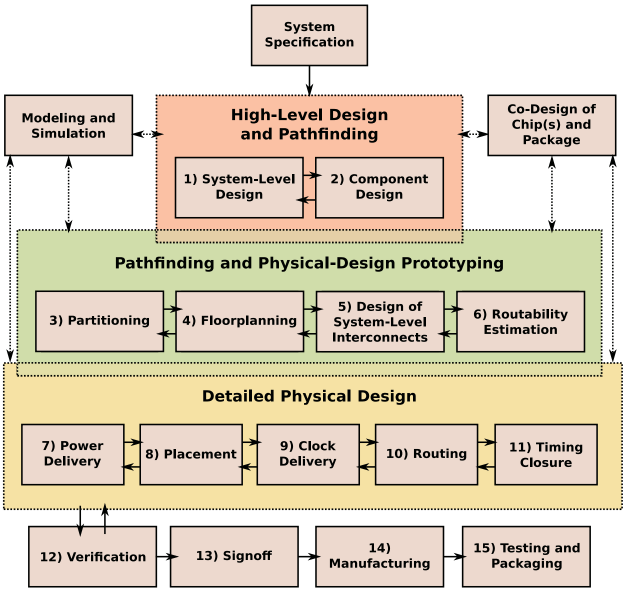


Fig. 4 Full workflow for custom design of 3D chips. Pathfinding and physical-design prototyping link system-level design and layout-level design; this link eases the design closure for the complex and highly iterative process. Modeling and simulation as well as chip-package co-design interact with most design stages. All stages require feedback loops to enable, among others, thermal management and stack-wide variation-aware design closure (not illustrated).

tion [63]. Still, interposer stacks are the most promising option for large-scale and system-level 3D integration.

1.2 On High-Level Challenges for the Design of 3D Chips

To select and explore the most suitable 3D integration option for any particular design is much more complex than handling similar decisions for classical 2D chips. A team of 3D designers has to consider the following aspects, among others:

- How to reuse intellectual property (IP) blocks or pre-designed modules effectively in the 3D chip in order to meet time-to-market and cost constraints?
- How are heterogeneous components designed and properly integrated along with digital modules?
- How can the final 3D chip be secured and made trustworthy?
- Into how many dies/layers should the overall design be split up, and how does the design perform after being spread across multiple dies/layers? How can a classical 2D implementation be leveraged as baseline for the 3D implementation [64]?
- What are the bandwidth, power, and signal integrity requirements for all the interconnects? What is an appropriate system-level interconnect fabric?
- How to test components/dies individually and the overall stack both partially and fully?

It is important to note that most of these aspects are interacting; consequently, any respective decision does impact the overall design process as well the final performance, reliability, and cost of the 3D chip. Solving such a complex set of intertwined challenges requires sophisticated design know-how, EDA capabilities and well-defined project structures. Given the plethora of available (2D) and upcoming (3D) tools, various design practices and design know-how, all distributed among multiple design parties, the introduction of a *unified workflow* is essential (**Fig. 4**).

For large-scale and system-level 3D integration—leveraging an interposer as “plug-and-play” integration backbone—much of the outlined design complexity and iteration processes may be kept under control or even avoided in the first place. That is, individual components/dies are designed and manufactured separately, and only then integrated into a 3D chip. Nevertheless, there are still design challenges (but also promising solutions) associated with this style, as we elaborate in the next sections.

2. Interposer Stacks: On Solutions and Future Prospects for Classical Design Automation

The physical design of interposer-based 3D-ICs is hampered by a multitude of design challenges that are similar to the ones encountered when designing other systems, such as system-on-a-package (SOP) or MCMs. Besides complexity, these are mainly issues of thermal, mechanical, and routability management. Testing issues also need special consideration (see Section 4); however, due to better access to individual dies, testing of interposer stacks is more manageable than it is for stacked 3D designs.

2.1 Floorplanning and Placement

As mentioned before, (technology-heterogeneous) chips are often designed independently and then placed on a silicon interposer. Hence, placement algorithms should arrange a small number (usually 2–10) of mostly bare dies on the interposer with the shortest external connections between them, in a manner analogous to classical floorplanning.

Today’s (academic) tools for die placement on interposer are often based on randomized algorithms such as *simulated annealing*, e.g., as proposed in Refs. [65], [66]. The authors of Ref. [67] apply an enumerative search to identify optimal die positions before using a pin assignment routine. This method, however, does not scale beyond six dies. The authors of Ref. [68] claim to effectively place the multiple FPGA dies of an interposer-based system. Based on force-directed placement and the *B*-tree* representation, their approach allows to optimize the die positions according to signal delay within the overall FPGA framework.

2.2 Data Structures and Solution Space

Design optimization is performed in the realm of the data structure’s *solution space* by applying some optimization algorithms. The algorithms require a solution space with minimum redundancy, excluding invalid solutions and including the best solutions. In addition, an efficient implementation of a data structure must allow for a fast execution of various operations. Examples are the exchange of components within and across multiple dies, the transformation from the abstract representation to the real 3D chip geometry, and the consideration of layout constraints.

The above requirements are notably harder to achieve for the 3D solution space than it has been in the case for “classical” 2D design automation [69], [70]. Still, efficient data structures initially developed for the physical design of 2D ICs (notably the *Slicing Tree*, the *O-Tree* or the *Sequence Pair*) have been successfully extended towards 3D integration. These extensions and other 3D data structures are reviewed in detail in Ref. [70].

2.3 Routability and Routing

Assuming that the dies to be integrated on the interposer are prefabricated, connecting (routing) them can be done with conventional routing tools. Hence, published work on routing concentrates on various interposer-specific constraints which are often technology-related. For an active interposer, however, the design of a large-scale and possibly hierarchical network-on-chip (NoC) requires further research efforts [61].

A global routing algorithm for SOPs is presented in Ref. [71]; it can also be applied to interposer systems for routing or routability estimation purposes. The authors of Ref. [72] studied the impact of IR-drop while routing the interposer and redistribution layers (RDL) of each die, along with simultaneous planning of micro-bumps and signal assignment. Their approach initially determines the number of micro-bumps required for each die, assigns I/O buffers, and finally routes the RDLs and the interposer. The minimization of the interposer's metal layers was sought after by the authors of Ref. [73]. Their approach is based on a routability estimation which then derives the minimum number of required metal layers.

2.4 Pin and TSV Assignment

During the aforementioned placement procedure, dies may change their relative positions and orientations which affect the individual and overall wirelength, due to non-optimal bump and/or pin assignment. Therefore, placement algorithms often include techniques for pin assignment. For example, the authors of Ref. [67] use a network-flow algorithm to establish the connections between I/O buffers and micro-bumps with the goal of minimizing the external wirelength. The approach in Ref. [66] applies *an integer-linear program* (*ILP*) formulation for the same purpose. Bipartite matching is leveraged in Ref. [65].

Alternatively, pin assignment can also be combined with the routing of dies. The authors of Ref. [72], for example, assign the I/O buffers (to the pre-placed bumps) prior to routing of the RDL and interposer layers. Their pin assignment is based on the optimization of network flows while also honoring IR-drop constraints.

2.5 Thermal Management

When compared to solely stacked 3D chips, interposer-based 3D chips also offer more flexible means for thermal management. Excessive thermal energy can dissipate more efficiently from the dies to the interposer (i.e., using the multiple heat paths via bumps), and it can also spread laterally and vertically to the outside/boundaries, where (multiple) heat sinks can be placed.

While a multitude of thermal-aware placement or floorplanning algorithms for stacked 3D designs have been published, there is a lack of similar solutions for interposer systems. Nevertheless, several thermal models and optimization flows are presented in Refs. [50], [74]. However, in order to facilitate a successful adoption for realistic interposer solutions, they need to be adapted and integrated into the early stages of the design flow, such as die placement or the floorplanning stage of the interposer circuit.

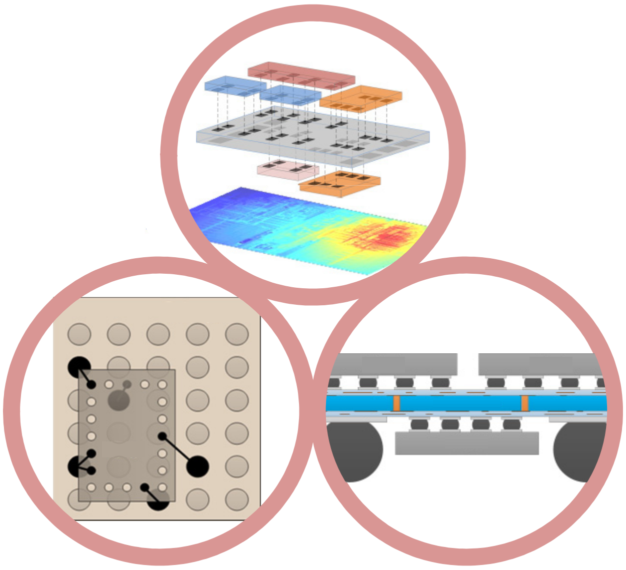


Fig. 5 Selected challenges for the design automation of interposer-based 3D chips: (top) holistic and package-wide thermal simulation, which shall also be fast, efficient, and accurate; (left) efficient and optimal die placement while considering/solving pin assignment; (right) chip-interposer co-design, exploring the technological and physical-design space of various interposer configurations.

2.6 Outlook: Novel Challenges for Design Automation

While interposer-based 3D chips are successfully designed and built using conventional but adapted design tools, there is still an urgent need for physical design methodologies that are tailored for the specific needs of interposer systems. Some of these challenges are outlined next (see also **Fig. 5**).

Multi-objective optimization during early design stages

Applying physical simulations or additional optimization goals during the early stages of physical design should enable the identification of the best-available solutions with state-of-the-art place and route algorithms. Specifically, routability estimation and thermo-mechanical simulations should be accounted for during the floorplanning and/or placement stages.

Chip-interposer co-design

The ultimate goal could be a simultaneous design of dies and interposer, that is, the design of the entire system within one flow (Fig. 4). This would enable the optimization of global key parameters like wirelength (external and internal), timing, routability and thermo-mechanical stability. However, such a system-level optimization might conflict with the aforementioned advantages of relatively easy heterogeneous integration, so its application has to be carefully calibrated considering all constraints.

Efficient and optimal die placement

The placement of dies has a significant effect on key interposer characteristics, such as performance. Since the number of dies is (so far) rather limited, it can be solved effectively or even optimally using tailored algorithms, even with pin assignment accounted for. However, most previous work applies probabilistic optimization [65], [66], which falls short of this prospect.

Fast thermal simulation

The inherently effective thermal management is one of the key advantages of interposer-based 3D design. To support this, fast thermal simulation should be integrated in the design flow for holistic estimation of thermal behavior during early design stages.

Data structures for large and heterogeneous 3D chips

Recall that data structures have been proposed for 3D physical-design automation. However, the heterogeneous structure of interposer-based 3D chips requires new and efficient data structures which take the special properties of interposer designs into account. Specifically, data structures that are capable of considering a multitude of constraints, such as inter-die thermal relationships, are needed. The concept of an *assembly design kit* (*ADK*) [75], which is analogous to the well-known PDK but tailored for 3D chips, is an interesting option towards this end.

3. Heterogeneous Interposer Stacks: Practical Solutions for Advanced Design Automation

One major benefit of the interposer architecture is that it enables a low-cost approach to heterogeneous integration with the possibility of placing photonics [76], MEMS [77], integrated power sources [78], imaging sensors [79] or acoustic transducers [80] on the same substrate as the IC dies. Furthermore, the interposer architecture enables novel ways for system integration based on vertical interconnect technologies that are not necessarily exclusively electrical [81], [82].

3.1 CAD Requirements

The major challenge in such heterogeneous system integration is that, by its very nature, it spans multiple physical domains. As a result, the design, analysis and verification of the heterogeneous system require that we augment the traditional VLSI CAD environment with several physics-aware features, including:

(1) Cross-domain design capabilities in general, with seamless interfaces between the various signal domains, be they electrical, mechanical, optical, acoustic, or fluidic.

(2) A rigorous methodology for signal-port definition and placement, capable of addressing each of the physical subsystems, to enable consistent interlocking between the state spaces of the various physical domains.

(3) A unified system-level language for describing the connectivity between various multi-port components belonging to different physical domains.

(4) A physics-aware verification framework enabling domain-aware design-rule checking and post-layout validation.

While the above features are needed even for 2D heterogeneous integration, the technological variety provided by the interposer architecture makes their incorporation in related CAD frameworks even more pressing. The interposer itself has additional requirements of its own that can be summarized as follows:

(1) Domain-aware planning and placement of vertical TSVs, be they electrical, optical, acoustic, or fluidic.

(2) Domain-aware design-rule checking of vertical interconnects, including keep-out zones, critical dimensions, and mechanical integrity rules.

(3) Domain-aware compact models of vertical interconnects to enable system-level performance evaluation.

An up-to-date account of the challenges faced in existing EDA environments in interposer-based, *electronic* integration is given in Ref. [83]. When such integration is *heterogeneous*, these challenges are compounded with additional complexities pertaining to the multi-physics nature of the heterogeneous case.

3.2 MEMS Integration

One possible way of dealing with these additional complexities is to "package them away" within the die itself, and to subsequently incorporate (on the interposer) an accordingly packaged die that has only electrical ports. This approach can be taken, e.g., for MEMS sensors where the electromechanical interface is encapsulated in the packaged die itself using wafer-scale, monolithic integration processes. Such MEMS processes are described in Refs. [84] and [77] for motion sensing, in Refs. [85] and [86] for ultrasound sensing, and in Ref. [87] for piezoelectric energy harvesting. Taking the latter process as a representative example, it is comprised of three bonded wafers with the middle one containing the mechanical element and the other two wafers constituting capping structures, bonded to the device wafer, with etched cavities to allow the mechanical element unconstrained movement.

In such MEMS devices where only their electrical pads are exposed to the interposer (e.g., capacitive accelerometers and gyroscopes, ultrasound transducers, piezoresistive pressure sensors, and piezoelectric energy harvesters), a physical and logical CAD methodology similar to the one advocated in Ref. [83] can be used. However, even under these favourable conditions, such a methodology will have to be adopted to the specific case of interposer-based MEMS integration, considering the following two caveats:

(1) The mechanical integrity of the MEMS devices in the presence of an interposer must be verified. Indeed, residual stresses induced by interposer bonding are bound to impact the mechanical figures of merit of the MEMS devices. In the case of resonant structures such as gyroscopes or magnetometers, both the resonant frequency and the Q factor can be impacted. In the case of an accelerometer, the maximum g acceleration rating of the device can be affected.

(2) In a bulk-machined, multi-wafer MEMS process, the MEMS devices are typically packaged and hermetically sealed under vacuum. The interposer-device assembly must be tested to verify that the MEMS device continues to meet design specifications post-bonding and that the device is still hermetically sealed.

Obviously, CMOS foundries have preference for MEMS processes that are CMOS-compatible, and the PDKs released for such processes are necessarily CMOS-centric. Due to the significant market opportunity of the Internet of Things (IoT), a consistent effort is being made by foundries and CAD vendors alike to provide the designers with comprehensive PDKs that include parameterized libraries for both IC and MEMS elements. Furthermore, the MEMS library elements are made visible to the IC design interface so that system-level co-simulations of the MEMS device and its interface ICs (i.e., the driver and readout) are enabled. This is for instance the case of the MEMS compact models produced by the *Coventor MEMS+* tool, which can be co-simulated with their respective ICs using *Cadence Spectre* within the *Virtuoso* analog design environment [88].

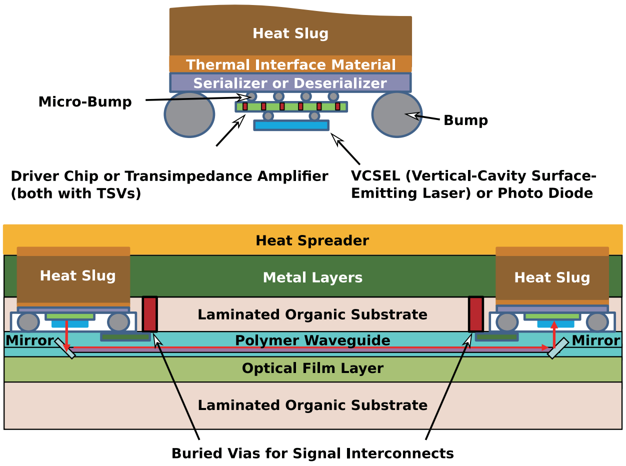

Heat Slug
Thermal Interface Material
Serializer or Deserializer
Micro-Bump
Bump
Driver Chip or Transimpedance Amplifier (both with TSVs)
VCSEL (Vertical-Cavity Surface-Emitting Laser) or Photo Diode
Heat Spreader
Heat Slug
Metal Layers
Heat Slug
Laminated Organic Substrate
Mirror
Polymer Waveguide
Mirror
Optical Film Layer
Laminated Organic Substrate
Buried Vias for Signal Interconnects

Fig. 6 An organic interposer supporting optoelectronic chips and embedded waveguides. Illustration derived from Ref. [8].

3.3 Photonics Integration

Unfortunately, in other interposer-based heterogeneous integration cases such as with photonics or micro-fluidics, the interposer will be presented with die ports that are not solely electrical. For instance, a Si photonic transceiver for fiber-optic data center communications will have optical ports as well as electrical ports. Coupling the optical ports to the interposer will necessitate passive photonics elements such as couplers and waveguides on the interposer itself. To enable such elements, the silicon interposer will have to include SOI cross sections similar to the ones supported by the 2D Si photonics platforms of *IBM* [89], *STMicroelectronics* [90], or *IME* [91].

Although these integration processes are fundamentally 2D, they can conceivably be adapted to a 3D stacking solution. A case in point is the 3D stacking of IC drivers on photonics components using a copper micro-pillar technology as in the *STMicroelectronics* process described in Ref. [92]. It is to be noted that this photonic-electronic integration is happening at the electrical interconnect level and, unlike the interposer solution of Ref. [81], no photonic TSVs are used. Conceivably, an electrical TSV can replace the micro pillar used in Ref. [92] if an interposer solution to IC-photonics 3D integration is adopted. But such TSV has the disadvantage that it will present a higher capacitance to the driver circuit, thus increasing the power consumption of the photonic transceiver. At the same time, the interposer can act as a heat spreader and alleviate the Joule heating due to the electronic driver. It is well known that photonic paths are extremely sensitive to thermal effects, and so the interposer solution in combination with an athermal photonic path design [93] will minimize the negative thermal impact. Another example is that of an organic interposer supporting optoelectronic chip communications using embedded mirrors and polymer waveguides as illustrated in **Fig. 6**. As in the MEMS case, CMOS foundries are in preference for such a monolithic CMOS-photonics integration.

From a CAD viewpoint, the heterogeneous design environment will be IC-centric with the reference design flows for the CMOS-photonics processes supporting passive and active photonic library elements. This has given rise to a new acronym in the EDA industry, namely, *EPDA*, which stands for Electronic/Photonic Design Automation. Here also, *Cadence's Virtuoso* can play the role of a heterogeneous design cockpit both on the front-end for system-level simulation (using, for instance, the *INTERCONNECT* tool from *Lumerical Solutions*) and on the back-end for physical design (using, for instance, *PhotoDesigner* from *PhoeniX Software*) [94]. The *Pyxis* custom design environment from *Mentor Graphics* can play a similar role. An emerging CAD feature, already implemented in *PhotoDesigner*, is automatic waveguide routing in the photonic domain. The extension of this feature to automatic routing in the presence of photonic TSVs is still an open problem.

3.4 CMOS Image Sensors

While photonic devices require that the interposer supports passive elements to couple the photonic signals to the package, CMOS imagers will require that the interposer supports the pixel array with active elements such as photodetectors to transform the incident photon energy into electrical signals. In an Si interposer, for example, a Si-Ge process to implement the photodetectors will be required. In fact, this process is similar to the one used in the CMOS-compatible Si photonics processes mentioned above. Another possible imager architecture is a passive interposer with electrical TSVs, connecting the pixel array through its access circuits to the analog and signal-processing back-ends, which will be placed on the other side of the interposer.

One motivation for moving CMOS imagers from a 3D TSV-based solution [95], [96] to an interposer solution is to integrate advanced imaging solutions such as stereo vision, surround view cameras, and embedded 3D imaging. The challenge to the interposer solution is certainly the TSV foundry momentum in this particular market segment. Indeed, according to Ref. [97], the market for CMOS imaging sensors will account for 63% of the TSV market in 2019, very much ahead of the second market segment, namely, 3D stacked DRAM, which will account for only 17%.

Given the importance of the CMOS imaging market in the 3D integration landscape, a CAD tool for evaluating and comparing the various 3D CMOS imager solutions according to the metrics of power, pixel-array area, resolution, sensitivity and cost would be highly desirable.

3.5 Outlook

We expect that the market opportunity of the IoT will drive innovation in the area of interposer integration for heterogeneous systems. The key reason is that the interposer occupies the sweet spot at the intersection of low cost and small footprint.

Our main concern is the business model of heterogeneous integration, namely, who will own the heterogeneous interposer? Is it the Si foundry or the packaging house? The IoT supply chain will decide this important question in due time. Until then, the CAD framework for 2.5D or 3D heterogeneous integration will continue to be CMOS-centric as this is where the industry is most heavily invested.

4. Design-for-Test and Testing in 3D Chips

In this section, we elaborate on the challenges in testing 3D chips and the recent efforts in tackling these challenges. Naturally, the research developments in 3D chip testing have been mostly in the form of adopting 2D chip testing methods, while there are particular aspects unique to 3D chips that have necessitated the development of novel solutions.

4.1 From 2D to 3D Chip Testing

Regardless of the underlying chip architecture, testing is fundamentally an access problem. The parts of a circuit that are most challenging to test are typically those that are buried deep inside the circuit. For 2D chips, *Design-for-Testability* (*DfT*) structures such as test points, scan cells, and wrapper cells have been used to improve access, and thus, testability. These structures help to (*i*) control nets that are otherwise difficult to reach from the primary inputs and (*ii*) observe nets that are otherwise difficult to monitor through the primary outputs. This way, deeply embedded logic can be "isolated" from its environment. Yet physical structures are further needed to effect the connection between this logic and the primary inputs/outputs. For this purpose, scan chains, *Test Access Ports* (*TAPs*) and *Test Access Mechanisms* (*TAMs*) have been used in 2D chips. These solutions have also been standardized via *IEEE Std 1149.1* [98] and *IEEE Std 1500* [99]. Through these structures, 2D chips have been tested by applying *test stimuli* and observing the responses. The test stimuli is obtained via *automated test pattern generation* (*ATPG*) tools, which target for faults representing physical defects.

Development of the test techniques in the context of 3D chips has necessitated an understanding of what is the same and what is different for 3D chips with respect to 2D chips. Only then can the structures or techniques from 2D chips be adopted for 3D chips and novel ones be developed as needed. For example, isolation and access for 3D chips can be effected by adopting solutions from *IEEE Std 1149.1* [98] and *IEEE Std 1500* [99], albeit with slight modifications. Tester probe access for wafers is significantly more challenging in 3D chips than in 2D chips due to structures such as micro-bumps, which are too small, too dense and too numerous. New defects emerge for 3D chips due to processing steps that did not exist in 2D chips, e.g., wafer thinning, alignment and bonding [100]. Micro-bumps in 3D chips are susceptible to open/bridging defects [101]. New decisions specific to 3D chips also complicate the test flow; there are multiple points at which 3D chips may have to be tested. These are pre-bond, mid-bond (partial stack), post-bond (pre-packaging) and final tests (post-packaging; final product), each with its own challenges.

4.2 Test Flow

In large-scale 3D chips, known-good dies are stacked together or are connected through an interposer. A single defective die in the stack or a defective interposer results in an unusable 3D chip. It is therefore crucial to determine the points in which test needs to be conducted, preventing the stacking/connection of good dies on top of defective dies/interposer. As each test incurs cost, the decisions as to at what point and how much testing is conducted affect the overall cost of the product. At the same time, detecting a defective die/interposer early on helps save the excessive cost of good dies stacked/connected with bad ones. An interposer, for example, is typically cheaper than dies, which necessitates the identification of a defective interposer to prevent it from being connected to good and valuable dies. Pre-bond and final testing are almost considered standard practice for 3D chips; mid-bond and post-bond tests are optional. Detailed test cost modeling and optimization techniques have been proposed in Ref. [102].

4.3 Pre-Bond Testing

To ensure the stacking/connection of known-good dies, pre-bond testing is necessary. One key challenge thereby is probing the micro-bumps; they are difficult to access using the probing technology available today. Another challenge is the handling of wafers at intermediate stages.

Various techniques have been proposed for the pre-bond testing of interposer. The use of *e-fuses* inside interposer has been proposed in Ref. [103] to connect/disconnect functional paths; test paths are then created to test the interposer through a small number of added test pads that can be probed. Other approaches include the use of additional dummy metal layers to create test loops [104] or contactless testing using thermal images [105]. These techniques aim at testing the vertical and horizontal interconnects within the interposer. Vertical interconnects may have break, void and pin-hole faults [106], while horizontal interconnects may have open, inter-bridge and inner-bridge faults [107].

The pre-bond testing of TSVs can be performed contactless via ring oscillators [108]. This way, the potential TSV defects, such as micro-voids and pin-holes, can be tested for.

The pre-bond testing of dies, in order to detect the defects inside a die, is similarly hampered by the challenge of probing micro-bumps. Solutions include contactless test [109] or inserting additional probing pads to non-bottom dies at the cost of increased area [110]. Another concern is whether to perform the test before or after wafer thinning [111]. Running tests before wafer thinning excludes defects due to thinning. Also, TSVs are still buried inside the substrate, and thus, cannot be tested easily. Testing after thinning, however, necessitates delicate probing.

4.4 Mid-Bond, Post-Bond, and Final Testing

During mid-bond and post-bond tests, mainly the TSV-based interconnects are targeted. Final testing, on the other hand, is the last quality screening step prior to shipping the product to customers; any part of the 3D chip should remain testable here [111].

TSV-based interconnects can be tested via dedicated test pattern generator structures to cover transition faults and shorts [112]. Though the number of interconnects is large, a few patterns can potentially test for all these faults. Direct face-to-face BEOL bonding, another bonding option implemented without TSVs [23], can be tested via dedicated built-in-self-test (BIST) transceivers [113]. These transceivers help to sense high-resistive interconnects, which indicate bonding failures [113].

Dies and the interposer can be tested only if die isolation and access mechanisms are in place. External test access is obtained via probing, typically at wafer-level, for pre-bond, mid-bond and post-bond tests, and via package pins in final test. Further on-chip structures are needed to isolate and access the interposer and the dies from the external I/Os. This access is defined by *IEEE Std P1838* [114], which is reviewed next.

4.5 Test Access: *IEEE Std P1838* [114]

IEEE Std P1838 is a standard under development that aims at providing a standardized 3D-DfT, to ensure the inter-operability of dies possibly obtained from different vendors. The standard has been largely developed by adopting structures from *IEEE Std 1149.1* [98] and *IEEE Std 1500* [99]. **Figure 7** illustrates the test access mechanisms in 3D and 2.5D/interposer chips.

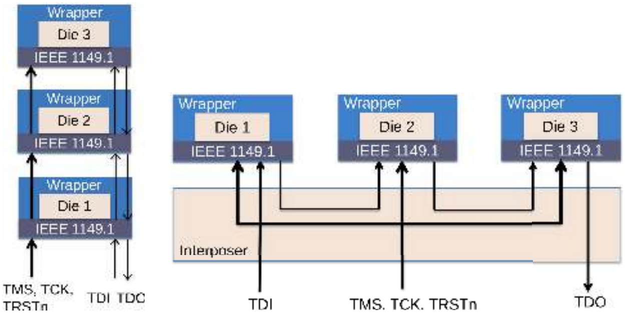
All dies are assumed to have *wrappers* around them similar to the wrapping of cores in *IEEE Std 1500*. The wrappers support *INTEST* operations where the internal die is tested, and *EXTEST* operations where the die interconnects (i.e., micro-bumps, TSVs, interposer connections) are tested while bypassing the dies. To do so, the wrappers support shift, capture, and apply operations.

Every die is assumed to have its TAP controller as in *IEEE Std 1149.1*; this serial control mechanism connects the dies along the stack (or through the interposer), providing them a one-bit bandwidth for testing as well. Bypass registers inside the dies allow the quick access of other dies or interconnects. The standard also supports a flexible n-bit parallel port to provide an optional parallel n-bit access to dies, enabling a high-bandwidth test as well.

4.6 Summary and Outlook

Testing of 3D (and 2D) chips is essentially characterized by the quest for speedy, comprehensive, yet low-cost access to all the internal circuitry. In contrast to 2D chips, 3D chips contain more components to be tested both individually and for the whole stack, rendering the test procedures more complex, costly, and iterative in nature. Furthermore, novel 3D interconnects (mainly the TSVs) introduce new types of faults. System-level integration on an interposer notably eases testing since individual dies, which are typically fully functional legacy dies, can be easily tested before bonding them onto the interposer. Besides, probing an interposer may be facilitated by dedicated test pads; highly-integrated, small-footprint 3D ICs are harder to probe in comparison.

Most testing efforts leverage and extend well-established 2D test features, such as *IEEE Std 1149.1* [98], to limit the cost and need for novel tools when testing 3D chips [107], [114]. An interesting consideration is whether these efforts allow to streamline the test of heterogeneous 3D interposer. That is, how to first standardize and then implement access mechanisms for dies with diverse analog, photonics, MEMS or other components, and how to synchronize these mechanisms with those on the logic dies—these are all open challenges.



(a) (b)

Fig. 7 Test access mechanisms as proposed in *IEEE Std P1838* [114] for (a) stacked 3D ICs and (b) interposer-based chips. For both configurations, *IEEE Std P1838* utilizes *IEEE Std 1149.1* [98] for access control and *IEEE Std 1500* [99] for the wrapper. The mechanisms rely on the following signals: TDI/TDO (test data input/output), TMS (test mode select), TCK (test clock), TRSTn (test reset not) [114].

Another challenge yet to be addressed is the potential for *security breaches* via the test infrastructure. That is, a malicious tester or end-user may try to misuse that infrastructure, seeking access to sensitive on-chip assets such as hard-coded software IP or security tokens [115]. Such potential misuse of the test infrastructure is only one security concern among others; in the next section we elaborate on the related challenges and opportunities for 3D chips in more detail.

5. Towards Trustworthy 3D Integration

Hardware is at the base of any information processing and, thus, hardware is per se the *root of trust* (**Fig. 8**). Among other considerations, this suggests that any chip can only be considered trustworthy if all the individual hardware components as well as the whole (2D/3D) chip have been thoroughly evaluated in terms of their actual, implemented functionality versus their intended, specified functionality [116], [117], [118], [119][*3]. One crucial concern here is the economics-driven trend to increasingly outsource various steps of the manufacturing flow, e.g., to outsourced semiconductor assembly and test (OSAT) parties [122]. We expect this trend to further intensify for the complex and diverse 3D integration landscape, thereby increasing the risk exposure for 3D chips. To address and manage this challenge of verification and other security-centric challenges, the notions of *"secure by design"* and *"design-for-trust"* have been promoted for some years now for "regular" 2D chips [116], [117], [118], [119], [123], [124], [125], [126], [127], [128]. Similar studies are recently focusing on 3D chips as well [129], [130], [131], [132], [133], [134], [135], [136], [137], [138]. Note that early stud-

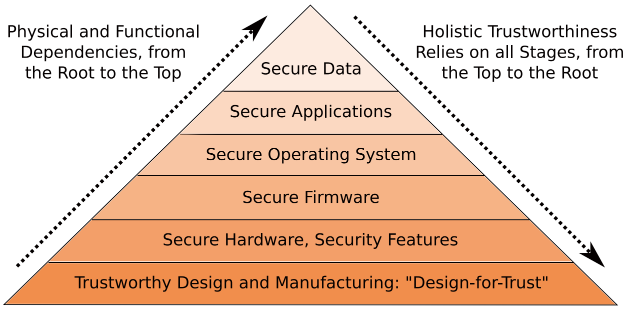

Physical and Functional Dependencies, from the Root to the Top
Holistic Trustworthiness Relies on all Stages, from the Top to the Root
Secure Data
Secure Applications
Secure Operating System
Secure Firmware
Secure Hardware, Security Features
Trustworthy Design and Manufacturing: "Design-for-Trust"

Fig. 8 Pyramid of security stages for modern (2D/3D) chips. Trustworthy information processing relies on all stages, and physical and functional dependencies are built up inherently from the root to the top. For example, the notion of secure hardware as *root of trust*—which also provides security features to enable secure processing further up the pyramid—relies itself on trustworthy design and manufacturing steps. "Design-for-trust" seeks to induce that essential trust in those very steps via a multitude of measures, such as *split manufacturing*.

[*3] Physical and functional verification traditionally has been (and still is) a major challenge for modern chip design itself [120], [121].

ies and whitepapers on 3D integration indicate the potential for trustworthy 3D chips as well [139], [140].

Here we review challenges and promising solutions towards trustworthy chips, both for 2D and 3D integration. Note that most solutions devised for 2D chips can be applied for 3D stacks as well, as long as the latter reuse some 2D components/dies (i.e., such 2D security solutions are not directly applicable for monolithic or full-custom 3D stacks). Additionally, we also highlight distinct aspects arising for 3D integration.

5.1 Securing the Test Infrastructure and Test Procedure

Recall that the test infrastructure may be misused by malicious testers/end-users [115]. Note that 3D chips may offer even new avenues for such attacks. For example, testing channels implemented by dedicated TSVs may leak data to other nearby, regular TSVs (or wires) via cross-coupling effects. More concerning, these effects may also be exploited to inject malicious data into the testing-channel TSVs via nearby "aggressor" TSVs. Cross-coupling effects have been generally accounted for [141], [142]; the outlined leakage/injection in TSVs can also be mitigated [133], albeit with considerable cost and effort. Still, only few studies explored such test-specific aspects for the security assessment of 3D chips so far; other risks may have been overlooked until now.

At the same time, 3D integration can help to secure the system-level test procedure, thanks to the die wrappers proposed in *IEEE Std P1838* [114]. That is because any sensitive information about the die's assets (required for ATPG) can be concealed from an untrusted OSAT party, assuming that the designers provide the test patterns along with the dies. Besides die wrappers, such a secure testing procedure would still require features like cryptographic primitives for protected and controlled access to the test infrastructure [143].

5.2 Verification of Outsourced Components

It is straightforward that the more outsourced components a 2D/3D chip contains, the higher the risk that some of them are faulty and/or prone to attacks. Components can be rendered unintentionally faulty/prone, via design or implementation bugs (e.g., *Rowhammer* [144]), but they can also be made intentionally and inherently faulty/prone (e.g., via *hardware Trojans* [145], see Section 5.4).

Recent work on structural and functional verification targets the security analysis of outsourced components [116], [117], [118], [119]. In general, for any 2D/3D chip, the efforts for verification scale with:

(1) the number of outsourced components;

(2) the structural and functional complexity of the outsourced components;

(3) the "permission for introspection" of outsourced components: soft IP components typically offer detailed insights and access into their implementation, whereas hard IP components tend to obfuscate such details; and

(4) the system-level connectivity of outsourced components intertwined with custom-designed components.

For large-scale 2D/3D integration, where typically most components are outsourced due to time-to-market constraints, it may become practically infeasible to verify the full 2D/3D chip. At the same time, one faulty/prone component may compromise the trustworthiness of the whole chip, necessitating that all components be monitored during runtime, as discussed next.

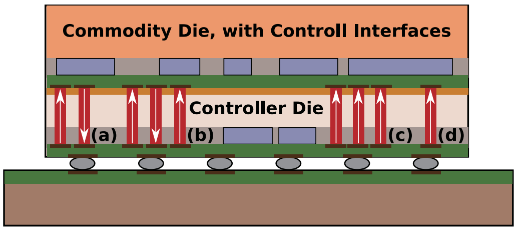


Fig. 9 Abstract scheme of Refs. [129], [130]. Each security feature requires an introspective interface (TSVs, in red) between the controller/security die and the untrusted commodity die, along with some additional transistors for the latter (not illustrated). The arrows in the TSVs indicate the signal flow, and the function of each feature is explained next (along with TSV references): (a) signal tapping, with on/off (left) and the actual signal (right); (b) re-routing, with on/off (left), the re-routed signal (middle), and off/on for the original signal (right); (c) overriding, with on/off (left), new signal on/off (middle), and the actual new signal (right); and (d) disabling, with on/off.

5.3 Runtime Attacks and Hardware Monitors

Malicious software or malicious end-user may seek to retrieve critical information from on-chip assets, either with or without the help of hardware Trojans. In the latter case, such attacks typically exploit some *side-channel information*, which reflects the various physical interactions that any electronic device experiences. For example, demonstrated attacks successfully leverage the spatio-temporal thermal patterns [146], [147] or the measurable timing behaviour [144] of modern chips. It is understandably hard—if possible at all—to anticipate all potential attacks on modern, large-scale, and more and more heterogeneous electronic devices. This implies a practical challenge: how to detect advanced and possibly yet unknown attacks at runtime?

With that challenge in mind, one particularly aspiring solution towards trustworthy chips are *hardware monitors* or *wrappers* for the continuous and pervasive control of untrusted and/or security-critical components [129], [130], [139], [148], [149], [150], [151]. The moment such monitors/wrappers observe some malicious behaviour, i.e., any behavioural anomaly with respect to well-defined, "normal" patterns (which may also be re-programmed if need arises), the related components are overridden or isolated. In order to compensate for the resulting "loss in processing capacity," redundant components may be provisioned for.

The notion of monitors is especially attractive in the context of 3D integration; untrustworthy components in one die may be controlled in a precise and localized manner with the help of monitoring components implemented in another die [129], [130], [139]. For example, Valamehr et al. [129], [130] propose powerful security features acting on the gate- and transistor-level, based on *introspective TSV interfaces* (**Fig. 9**). These features allow for tapping, overriding, re-routing, and disabling of internal signals at will.

5.4 Detection of Hardware Trojans

Hardware Trojans are another major concern for reliable and trustworthy chips; they are hardware modifications inserted by an untrustworthy third party in order to alter the chip's functionality, leak critical information, or degrade the chip's reliability and/or performance [145]. The detection of hardware Trojans, both at design and runtime, has recently gained more interest, and promising techniques have been proposed [116], [117], [118], [119], [145], [148], [152], [153]. For example, simulation-based Trojan detection cannot guarantee full coverage within polynomial runtime, but Wei et al. [153] demonstrate full coverage for industrial circuits within minutes by combining reverse engineering and formal verification. Still, advanced Trojans will be extremely hard to detect; they may, for example, exhibit no distinguishable patterns at all during functional analysis [127].

Note that hardware monitors (Section 5.3) may also be used for the runtime detection of Trojans. As indicated, this is especially attractive for 3D chips where such monitors can be implemented in trustworthy dies, separated from the potentially Trojan-infected legacy chips [127], [129], [130], [139]. Nevertheless, some Trojans may be crafted specifically for 3D integration and end up being "buried somewhere in the midst of the 3D chip"; they are harder to detect during runtime [134], and may also exploit distinct trigger mechanisms such as increased internal heating [154].

5.5 Split Manufacturing

Another recent approach towards trustworthy chips is *split manufacturing* [124], [135], [140], [155], [156], [157], [158], [159], [160], [161], [162]. It seeks to prevent the insertion of Trojans and/or the theft of IP in the first place.

More specifically, the key idea is to split the manufacturing process into several parts, typically as follows: (*i*) the advanced and high-end FEOL parts, which are costly to manufacture and are thus typically outsourced; and (*ii*) the "modest" BEOL parts, which are relatively cheap to manufacture in low-end but trusted fabs. To the untrusted FEOL party, the outsourced design parts merely appear as a "sea of gates," where the missing interconnects *may* prevent one from (*i*) inferring any of the actual functionality and/or (*ii*) localizing particular circuitry prone or fruitful for Trojan attacks. How exactly such splitting can be rendered truly secure yet practical (in terms of reasonably low manufacturing and layout-level cost) is currently still under broad and vivid investigation [155], [156], [157], [159], [160], [161].

Note that split manufacturing for 3D chips (3D SM) is more flexible and, thus, potentially more secure than for 2D chips, at least in theory [162]. That is because 3D integration allows to split a design into multiple 2D dies, which then represent independent FEOL/BEOL parts. Some or all of the BEOL parts may also be manufactured only by the trusted party [124], [140]. Especially interposer-based 3D SM is hence promising, since it allows to keep some BEOL parts confidential for the final stacking process in the trusted fab [135], [155], [158]. In practice, however, there are some constraints for 3D SM:

- Test and diagnosis of 3D chips (Section 4) typically mandates that individual dies be pre-bond tested. This implies that any split of FEOL/BEOL parts across the 3D stack shall maintain the testability of individual dies; this is an open challenge. As of now, classical known-good die testing limits 3D SM towards 2D SM and possibly easy to resolve layouts, which is contradicting the original promise of 3D SM.
- There is an inherent trade-off between security and cost imposed by 2D/3D SM. When FEOL and BEOL parts are split across large distances among multiple dies and/or an interposer, the impact on power, performance, and area will be more exaggerated than for 2D SM. Previous work on 3D SM either oversimplified this challenge [158] or explored only the scope of secure-but-excessive-overhead solutions [155].
- For up-and-coming monolithic 3D chips, manufacturing is typically conducted in a single high-end fab, precluding 3D SM altogether. Similarly, for 3D SM with advanced TSV-based 3D chips, the requirements on high-precision alignment, bonding, and stacking may be met only by a few, potentially untrustworthy OSAT parties.

In essence, 3D SM may not be superior to "classical" 2D SM, at least not unless it is performed holistically, considering the trade-offs for cost and security as well as the prospects for splitting at the chip- and/or the system-level of 3D stacks.

5.6 Summary and Outlook

Notwithstanding the claims made in prior work regarding security (by allegedly providing a proper *root of trust*), most work relies on naive, overly optimistic assumptions regarding their design and implementation. For example, it is easy to see that hardware monitors/wrappers (Section 5.3) are particularly prone to Trojan-based attacks. The moment third parties are involved in the design and/or manufacturing process of chips containing such monitors/wrappers, these parties must be trustworthy. Otherwise, the implementation and functionality of the security features themselves cannot be trusted in the first place.

Remarkably, this concern also applies to 3D integration where untrustworthy commodity components and trusted monitor/supervisor components can be easily manufactured in different dies (or across an interposer) for security reasons [129], [130], [135], [139]. In order to monitor an untrusted die (without leveraging side-channel information), the separate supervisor die has to rely on the proper physical and functional implementation of some introspective interfaces built within the commodity die. For example, recall that Valamehr et al. [129], [130] propose several security features which all rely on such interfaces (Fig. 9). These features may easily fail or be mislead with false data/signals in case the interfaces are manipulated by untrusted third parties involved for the design and manufacturing of the commodity dies.

In essence, it is arguably difficult yet essential to avoid *insecure physical and functional dependencies* where security features rely on untrusted components and/or third parties to perform their intended security functions. If this key requirement fails, the whole root of trust is inevitably undermined (Fig. 8).

System-level 3D integration appears promising towards this end. Here, any untrustworthy component/die shall depend on a *trustworthy system platform* (e.g., an actively secured interposer, see **Fig. 10**) for its system-level applicability, and not vice versa.

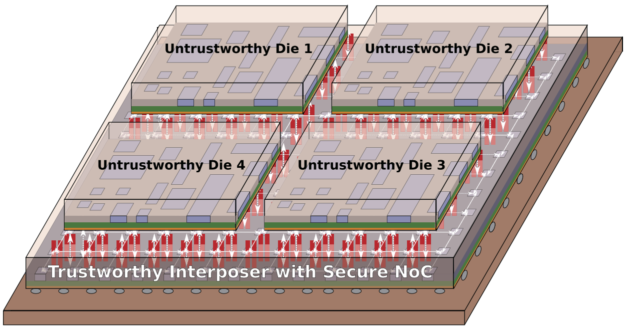


Fig. 10 A large-scale and trustworthy, interposer-based 3D chip. The active interposer with the secure network-on-chip (NoC) is the backbone, i.e., the *root of trust*. Any internal communication is to remain within the untrustworthy dies to limit the load on the interposer NoC; system-wide and external communication has to be routed through the secure NoC. In case malicious traffic coming from an untrustworthy die is detected by the secure NoC, the respective die is isolated, i.e., decoupled from the NoC. Isolating only the malicious component(s) instead of the whole die is not practical—we cannot rely on any control features implemented in that die to begin with, as the malicious component(s) may undermine them as well.

As this approach is implementing a thorough root of trust along with a correct dependency scheme, it becomes relatively easy to detect and properly isolate malicious components from the trustworthy 3D system if need arises. Note that isolating malicious dies implies no compromise for the system's overall security, but "only" a loss of functionality. The latter can be provisioned for, at least to some degree, by integrating functionally redundant yet physically different commodity dies (from different vendors).

6. Summary and Conclusion

In this paper, we discuss the state-of-art for 3D integration, with particular focus on design automation, testing, and trustworthy system integration. We review the most relevant challenges, we outline existing and promising solutions, and we point out needs for further research and development. In the following we summarize the key points of this paper.

3D implementation options: The sequentially manufactured monolithic 3D ICs enable the highest integration density (i.e., transistor-level 3D integration) but require full-custom design which largely hinders design reuse. Furthermore, monolithic 3D ICs are so far demonstrated only for the digital domain. TSV-based 3D ICs enable chip-level integration of both homogeneous and heterogeneous components but still require a unified 3D design flow and dedicated manufacturing steps. Interposer stacks allow for "plug-and-play" reuse of legacy 2D chips and are thus the most promising option for large-scale 3D integration; interposer have been widely accepted and applied in the industry by now. Still, there are currently unresolved needs, e.g., for design automation and test of heterogeneous interposer stacks. Finally recall that advanced 3D stacks may combine different options, such as multiple TSV-based 3D ICs integrated on an interposer.

Design automation: The design of 3D chips becomes increasingly difficult and demanding as compared to well-engineered solutions for 2D chips. That is mainly due to the plethora of complex design decisions to make (such as how to reuse digital and/or heterogeneous IP components, or how to organize the overall 3D chip) and the highly iterative design flow. For full-custom 3D designs, the stages of system-level design, design prototyping, and detailed physical design are all intertwined and furthermore require advanced capabilities, e.g., for chip-package co-design. While more and more 3D design-automation solutions are becoming available (also with 2D tools being extended), there is still a need for dedicated tools to design particular applications such as CMOS imaging sensors.

Testing: Both the test of individual components/dies as well as the test of the full 3D chip is required; the former is to ensure integration of known-good dies while the latter is to ensure the proper 3D interconnectivity and the overall functionality. On the one hand, existing probing technology falls short in providing physical access to dies/interposer through micro-bumps, complicating the test of 3D chips. On the other hand, well-established 2D testing standards are currently being extended towards 3D testing, streamlining the efforts for testing. Besides, standardized access mechanisms for not purely digital but heterogeneous 3D stacks are currently also still lacking.

Trustworthy integration: Secure hardware is at the heart of any trustworthy information processing, also in up-and-coming 3D chips. While recent advances for "classical 2D hardware security" can be leveraged for 3D chips to some degree, 3D chips present unique challenges as well as opportunities. For example, security measures such as split manufacturing may benefit from the additional third dimension but also need to comply with practical constraints, e.g., testability and performance of split dies. Another important consideration is that TSVs experience cross-coupling effects which may be exploited to leak on-chip assets and/or tamper with the data at runtime. Finally, system-level 3D integration on an active interposer can, arguably for the first time, enable truly trustworthy integration of untrusted components.

Conclusion: 3D integration has been advocated and explored by industry and academia for many years now. While there is still a multitude of challenges for various aspects of 3D integration, there is also notable progress, and different products (memory-centric 3D ICs, large-scale 3D FPGAs, NoC interposer, etc.) are already in high volumes in the market. Besides the TSV-based 3D ICs, which have been highly anticipated early on, the more practical, cost-effective and flexible interposer stacks may eventually dominate the 3D landspace. Aside from the easy heterogeneous integration using interposer, this is also because interposer can serve as a "unifying integration backbone" for both classical, legacy 2D chips as well as novel, fully customized 3D ICs.

Acknowledgments The authors thank Sergii Osmolovskyi (TU Dresden) for his input on interposer integration (Section 2).

References

[1] Patti, R.S.: Three-Dimensional Integrated Circuits and the Future of System-on-Chip Designs, *Proc. IEEE*, Vol.94, No.6, pp.1214–1224 (online), DOI: 10.1109/JPROC.2006.873612 (2006).

[2] Borkar, S.: 3D Integration for Energy Efficient System Design, *Proc. Des. Autom. Conf.*, pp.214–219 (online), DOI: 10.1145/2024724.2024774 (2011).

[3] Lim, S.K.: *Design for High Performance, Low Power, and Reliable 3D Integrated Circuits*, Springer (online), DOI: 10.1007/978-1-4419-9542-1 (2013).

[4] Arden, W., Brillouët, M., Cogez, P., et al.: "More-than-Moore" White Paper, Technical report, ITRS (online), available from ⟨http://www.itrs2.net/uploads/4/9/7/7/49775221/irc-itrs-mtm-v2_3.pdf⟩

(2010).

[5] JEDEC Solid State Technology Association: JEDEC Standard: JESD235A High Bandwidth Memory (HBM), (online), available from ⟨http://www.jedec.org/standards-documents/docs/jesd235a⟩ (2015).

[6] SK HYNIX INC.: SK Hynix HBM Graphics Memory, (online), available from ⟨http://www.skhynix.com/inc/pdfDownload.jsp?path=/datasheet/Databook/Databook_Q4'2014_Graphics.pdf⟩ (2014).

[7] Banerjee, K., Souri, S.J., Kapur, P., et al.: 3-D ICs: A Novel Chip Design for Improving Deep-Submicrometer Interconnect Performance and Systems-on-Chip Integration, *Proc. IEEE*, Vol.89, No.5, pp.602–633 (online), DOI: 10.1109/5.929647 (2001).

[8] Lau, J.H.: The Most Cost-Effective Integrator (TSV Interposer) for 3D IC Integration System-in-Package (SiP), *Proc. ASME InterPACK*, pp.53–63 (online), DOI: 10.1115/IPACK2011-52189 (2011).

[9] Knechtel, J. and Lienig, J.: Physical Design Automation for 3D Chip Stacks – Challenges and Solutions, *Proc. Int. Symp. Phys. Des.*, pp.3–10 (online), DOI: 10.1145/2872334.2872335 (2016).

[10] Todri-Sanial, A. and Tan, C.S. (Eds.): *Physical Design for 3D Integrated Circuits*, CRC Press, Taylor & Francis (online), available from ⟨https://www.crcpress.com/Physical-Design-for-3D-Integrated-Circuits/Todri-Sanial-Tan/p/book/9781498710367⟩ (2016).

[11] Elfadel, I.A.M. and Fettweis, G. (Eds.): *3D Stacked Chips – From Emerging Processes to Heterogeneous Systems*, Springer (online), DOI: 10.1007/978-3-319-20481-9 (2016).

[12] Radojcic, R.: *More-than-Moore 2.5D and 3D SiP Integration*, Springer (online), DOI: 10.1007/978-3-319-52548-8 (2017).

[13] Lu, T., Serafy, C., Yang, Z., et al.: TSV-based 3D ICs: Design Methods and Tools, *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, Vol.PP, No.99, pp.1–1 (online), DOI: 10.1109/TCAD.2017.2666604 (2017).

[14] Van der Plas, G., Limaye, P., Loi, I., et al.: Design Issues and Considerations for Low-Cost 3-D TSV IC Technology, *J. Sol.-St. Circ.*, Vol.46, No.1, pp.293–307 (online), DOI: 10.1109/JSSC.2010.2074070 (2011).

[15] Vaisband, B. and Friedman, E.G.: Noise Coupling Models in Heterogeneous 3-D ICs, *Trans. VLSI Syst.*, Vol.24, No.8, pp.2778–2786 (online), DOI: 10.1109/TVLSI.2016.2535370 (2016).

[16] Kumar, G., Bandyopadhyay, T., Sukumaran, V., et al.: Ultra-high I/O density glass/silicon interposers for high bandwidth smart mobile applications, *Proc. Elec. Compon. Tech. Conf.*, pp.217–223 (online), DOI: 10.1109/ECTC.2011.5898516 (2011).

[17] Zhang, C. and Sun, G.: Fabrication cost analysis for 2D, 2.5D, and 3D IC designs, *Proc. 3D Sys. Integ. Conf.*, pp.1–4 (online), DOI: 10.1109/3DIC.2012.6263032 (2012).

[18] Takaya, S., Nagata, M., Sakai, A., et al.: A 100GB/s wide I/O with 4096b TSVs through an active silicon interposer with in-place waveform capturing, *Proc. Int. Sol.-St. Circ. Conf.*, pp.434–435 (online), DOI: 10.1109/ISSCC.2013.6487803 (2013).

[19] Kannan, A., Jerger, N.E. and Loh, G.H.: Enabling Interposer-based Disintegration of Multi-core Processors, *Proc. Int. Symp. Microarch.*, pp.546–558 (online), DOI: 10.1145/2830772.2830808 (2015).

[20] Yoshida, J.: Leti Unveils New 3D Network-on-Chip - 'Smart' Interposer drives high-perfomance, low-energy 3D IC, (online), available from ⟨http://www.eetimes.com/document.asp?doc_id=1330129⟩ (2016).

[21] Clermidy, F., Vivet, P., Dutoit, D., et al.: New perspectives for multicore architectures using advanced technologies, *Proc. Int. Elec. Devices Meeting*, pp.35.1.1–35.1.4 (online), DOI: 10.1109/IEDM.2016.7838545 (2016).

[22] Stow, D., Akgun, I., Barnes, R., et al.: Cost Analysis and Cost-driven IP Reuse Methodology for SoC Design Based on 2.5D/3D Integration, *Proc. Int. Conf. Comp.-Aided Des.*, pp.56:1–56:6 (online), DOI: 10.1145/2966986.2980095 (2016).

[23] Beyne, E.: The 3-D Interconnect Technology Landscape, *J. Des. Test*, Vol.33, No.3, pp.8–20 (online), DOI: 10.1109/MDAT.2016.2544837 (2016).

[24] Yole Développement: Fan-Out: Technologies & Market Trends 2016, (online), available from ⟨https://www.i-micronews.com/report/product/fan-out-technologies-market-trends-2016.html⟩ (2016).

[25] Mahajan, R. and Sane, S.: Microelectronic package containing silicon patches for high density interconnects, and method of manufacturing same, Intel Corporation, (online), available from ⟨https://www.google.com/patents/US8064224⟩ (2011).

[26] Mahajan, R., Sankman, R., Patel, N., et al.: Embedded Multi-die Interconnect Bridge (EMIB) – A High Density, High Bandwidth Packaging Interconnect, *Proc. Elec. Compon. Tech. Conf.*, pp.557–565 (online), DOI: 10.1109/ECTC.2016.201 (2016).

[27] Deo, M.: Enabling Next-Generation Platforms Using Intel's 3D System-in-Package Technology, Technical report, Intel Corporation (online), available from ⟨https://www.altera.com/content/dam/altera-www/global/en_US/pdfs/literature/wp/wp-01251-enabling-nextgen-with-3d-system-in-package.pdf⟩ (2017).

[28] Kim, D.H., Athikulwongse, K., Healy, M.B., et al.: 3D-MAPS: 3D Massively Parallel Processor with Stacked Memory, *Proc. Int. Sol.-St. Circ. Conf.*, pp.188–190 (online), DOI: 10.1109/ISSCC.2012.6176969 (2012).

[29] Neela, G. and Draper, J.: Logic-on-logic partitioning techniques for 3-dimensional integrated circuits, *Proc. Int. Symp. Circ. Sys.*, pp.789–792 (online), DOI: 10.1109/ISCAS.2013.6571965 (2013).

[30] Thorolfsson, T., Lipa, S. and Franzon, P.D.: A 10.35 mW/GFlop stacked SAR DSP unit using fine-grain partitioned 3D integration, *Proc. Cust. Integ. Circ. Conf.*, pp.1–4 (online), DOI: 10.1109/CICC.2012.6330589 (2012).

[31] Vivet, P., Thonnart, Y., Lemaire, R., et al.: A 4x4x2 homogeneous scalable 3D network-on-chip circuit with 326MFlit/s 0.66pJ/b robust and fault-tolerant asynchronous 3D links, *Proc. Int. Sol.-St. Circ. Conf.*, pp.146–147 (online), DOI: 10.1109/ISSCC.2016.7417949 (2016).

[32] Tummala, R.R.: *System on Package: Miniaturization of the Entire System*, McGraw-Hill Professional (online), DOI: 10.1036/0071459065 (2008).

[33] Zhang, C. and Li, L.: Characterization and Design of Through-Silicon Via Arrays in Three-Dimensional ICs Based on Thermomechanical Modeling, *Trans. Electron Dev.*, Vol.58, No.2, pp.279–287 (online), DOI: 10.1109/TED.2010.2089987 (2011).

[34] Knechtel, J., Markov, I.L. and Lienig, J.: Assembling 2-D blocks into 3-D chips, *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, Vol.31, No.2, pp.228–241 (online), DOI: 10.1109/TCAD.2011.2174640 (2012).

[35] Chan, Y.S., Li, H.Y. and Zhang, X.: Thermo-Mechanical Design Rules for the Fabrication of TSV Interposers, *Trans. Compon., Pack., Manuf. Tech.*, Vol.3, No.4, pp.633–640 (online), DOI: 10.1109/TCPMT.2012.2223758 (2013).

[36] Knechtel, J., Young, E.F.Y. and Lienig, J.: Planning Massive Interconnects in 3-D Chips, *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, Vol.34, No.11, pp.1808–1821 (online), DOI: 10.1109/TCAD.2015.2432141 (2015).

[37] Nandakumar, V.S. and Marek-Sadowska, M.: Layout Effects in Fine-Grain 3-D Integrated Regular Microprocessor Blocks, *Proc. Des. Autom. Conf.*, pp.639–644 (online), DOI: 10.1145/2024724.2024871 (2011).

[38] ITRS: International Technology Roadmap for Semiconductor, (online), available from ⟨http://www.itrs.net/Links/2009ITRS/Home2009.htm⟩ (2009).

[39] Lee, Y.-J. and Lim, S.K.: Ultrahigh Density Logic Designs Using Monolithic 3-D Integration, *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, Vol.32, No.12, pp.1892–1905 (online), DOI: 10.1109/TCAD.2013.2273986 (2013).

[40] Panth, S., Samadi, K., Du, Y., et al.: Shrunk-2D: A Physical Design Methodology to Build Commercial-Quality Monolithic 3D ICs, *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, Vol.PP, No.99, pp.1–1 (online), DOI: 10.1109/TCAD.2017.2648839 (2017).

[41] Shi, D. and Davoodi, A.: Improving Detailed Routability and Pin Access with 3D Monolithic Standard Cells, *Proc. Int. Symp. Phys. Des.*, pp.107–112 (online), DOI: 10.1145/3036669.3036676 (2017).

[42] Batude, P., Vinet, M., Previtali, B., et al.: Advances, challenges and opportunities in 3D CMOS sequential integration, *Proc. Int. Elec. Devices Meeting*, pp.7.3.1–7.3.4 (online), DOI: 10.1109/IEDM.2011.6131506 (2011).

[43] Samal, S.K., Samadi, K., Kamal, P., et al.: Full Chip Impact Study of Power Delivery Network Designs in Gate-Level Monolithic 3D ICs, *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, Vol.PP, No.99 (online), DOI: 10.1109/TCAD.2016.2616377 (2017).

[44] Budhathoki, P., Knechtel, J., Henschel, A., et al.: Integrating 3D Floorplanning and Optimization of Thermal Through-Silicon Vias, *3D Stacked Chips – From Emerging Processes to Heterogeneous Systems*, Elfadel, I.A.M. and Fettweis, G. (Eds.), chapter 10, Springer (online), DOI: 10.1007/978-3-319-20481-9 (2016).

[45] Samal, S.K., Panth, S., Samadi, K., et al.: Adaptive Regression-Based Thermal Modeling and Optimization for Monolithic 3-D ICs, *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, Vol.35, No.10, pp.1707–1720 (online), DOI: 10.1109/TCAD.2016.2523983 (2016).

[46] Park, J.-H., Shakouri, A. and Kang, S.-M.: Fast Thermal Analysis of Vertically Integrated Circuits (3-D ICs) Using Power Blurring Method, *Proc. ASME InterPACK*, pp.701–707 (online), DOI: 10.1115/InterPACK2009-89072 (2009).

[47] Billoint, O., Sarhan, H., Rayane, I., et al.: A comprehensive study of Monolithic 3D cell on cell design using commercial 2D tool, *Proc. Des. Autom. Test Europe*, pp.1192–1196 (online), DOI: 10.7873/DATE.2015.1110 (2015).

[48] Chang, K., Sinha, S., Cline, B., et al.: Cascade2D: A Design-aware Partitioning Approach to Monolithic 3D IC with 2D Commercial Tools, *Proc. Int. Conf. Comp.-Aided Des.*, pp.130:1–130:8 (online),

DOI: 10.1145/2966986.2967013 (2016).

[49] Samal, S.K., Nayak, D., Ichihashi, M., et al.: Monolithic 3D IC vs. TSV-based 3D IC in 14nm FinFET technology, *Proc. SOI-3D-Subthresh. Microel. Tech. Unified Conf.*, pp.1–2 (online), DOI: 10.1109/S3S.2016.7804405 (2016).

[50] Heinig, A., Fischbach, R. and Dittrich, M.: Thermal analysis and optimization of 2.5D and 3D integrated systems with Wide I/O memory, *Proc. Therm. Thermomech. Phen. Elect. Syst. Conf.*, pp.86–91 (online), DOI: 10.1109/ITHERM.2014.6892268 (2014).

[51] Fischbach, R., Lienig, J. and Meister, T.: From 3D circuit technologies and data structures to interconnect prediction, *Proc. Int. Worksh. Sys.-Level Interconn. Pred.*, pp.77–84 (online), DOI: 10.1145/1572471.1572485 (2009).

[52] Lenihan, T.G. and Vardaman, E.J.: Challenges to Consider in Organic Interposer HVM, *TechSearch Int. for iNEMI Substrate & Packaging Workshop*, (online), available from ⟨http://thor.inemi.org/webdownload/2014/Substrate_Pkg_WS_Apr/08_TechSearch.pdf⟩ (2014).

[53] Iyer, S.S.: Three-dimensional integration: An industry perspective, *MRS Bulletin*, Vol.40, No.3, pp.225–232 (online), DOI: 10.1557/mrs.2015.32 (2015).

[54] Khan, N., Yu, L.H., Pin, T.S., et al.: 3-D Packaging With Through-Silicon Via (TSV) for Electrical and Fluidic Interconnections, *Trans. Compon., Packag., Manuf. Technol.*, Vol.3, No.2, pp.221–228 (online), DOI: 10.1109/TCPMT.2012.2186297 (2013).

[55] Akgun, I., Zhan, J., Wang, Y., et al.: Scalable Memory Fabric for Silicon Interposer-Based Multi-Core Systems, *Proc. Int. Conf. Comp. Des.*, pp.33–40 (online), DOI: 10.1109/ICCD.2016.7753258 (2016).

[56] Macri, J.: AMD's next generation GPU and high bandwidth memory architecture: FURY, *Hot Chips Symp.*, pp.1–26 (online), DOI: 10.1109/HOTCHIPS.2015.7477461 (2015).

[57] Smith, R.: The Fiji GPU: Go Big or Go Home, (online), available from ⟨http://www.anandtech.com/print/9390/the-amd-radeon-r9-fury-x-review⟩ (2015).

[58] Lee, C.C., Hung, C., Cheung, C., et al.: An Overview of the Development of a GPU with Integrated HBM on Silicon Interposer, *Proc. Elec. Compon. Technol. Conf.*, pp.1439–1444 (online), DOI: 10.1109/ECTC.2016.348 (2016).

[59] Dorsey, P.: Xilinx Stacked Silicon Interconnect Technology Delivers Breakthrough FPGA Capacity, Bandwidth, and Power Efficiency, Technical report, Xilinc, Inc. (online), available from ⟨https://www.xilinx.com/support/documentation/white_papers/wp380_Stacked_Silicon_Interconnect_Technology.pdf⟩ (2010).

[60] Milojevic, D., Marchal, P., Marinissen, E.J., et al.: Design issues in heterogeneous 3D/2.5D integration, *Proc. Asia South Pac. Des. Autom. Conf.*, pp.403–410 (online), DOI: 10.1109/ASPDAC.2013.6509630 (2013).

[61] Loh, G.H., Jerger, N.E., Kannan, A., et al.: Interconnect-Memory Challenges for Multi-chip, Silicon Interposer Systems, *Proc. MEMSYS*, pp.3–10 (online), DOI: 10.1145/2818950.2818951 (2015).

[62] Yao, W., Pan, S., Achkir, B., et al.: Modeling and Application of Multi-Port TSV Networks in 3-D IC, *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, Vol.32, No.4, pp.487–496 (online), DOI: 10.1109/TCAD.2012.2228740 (2013).

[63] Martin, B., Han, K. and Swaminathan, M.: A Path Finding Based SI Design Methodology for 3D Integration, *Proc. Elec. Compon. Tech. Conf.*, pp.2124–2130 (online), DOI: 10.1109/ECTC.2014.6897596 (2014).

[64] Chan, W.-T., Du, Y., Kahng, A., et al.: 3DIC Benefit Estimation and Implementation Guidance from 2DIC Implementation, *Proc. Des. Autom. Conf.*, pp.30:1–30:6 (online), DOI: 10.1145/2744769.2744771 (2015).

[65] Ho, Y.-K. and Chang, Y.-W.: Multiple chip planning for chip-interposer codesign, *Proc. Des. Autom. Conf.*, pp.27:1–27:6 (online), DOI: 10.1145/2463209.2488767 (2013).

[66] Seemuth, D., Davoodi, A. and Morrow, K.: Automatic die placement and flexible I/O assignment in 2.5D IC design, *Proc. Int. Symp. Quality Elec. Des.*, pp.524–527 (online), DOI: 10.1109/ISQED.2015.7085480 (2015).

[67] Liu, W.-H., Chang, M.-S. and Wang, T.-C.: Floorplanning and Signal Assignment for Silicon Interposer-based 3D ICs, *Proc. Des. Autom. Conf.*, pp.5:1–5:6 (online), DOI: 10.1145/2593069.2593142 (2014).

[68] Mao, F., Zhang, W., Feng, B., et al.: Modular placement for interposer based multi-FPGA systems, *Proc. Great Lakes Symp. VLSI*, pp.93–98 (online), DOI: 10.1145/2902961.2903025 (2016).

[69] Wang, R., Young, E.F.Y. and Cheng, C.-K.: Complexity of 3-D floorplans by analysis of graph cuboidal dual hardness, *Trans. Des. Autom. Elec. Sys.*, Vol.15, No.4, pp.33:1–33:22 (online), DOI: 10.1145/1835420.1835426 (2010).

[70] Fischbach, R., Lienig, J. and Knechtel, J.: Investigating modern layout representations for improved 3D design automation, *Proc. Great Lakes Symp. VLSI*, pp.337–342 (online), DOI: 10.1145/1973009.1973076 (2011).

[71] Minz, J.R. and Lim, S.K.: Block-level 3-D Global Routing With an Application to 3-D Packaging, *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, Vol.25, No.10, pp.2248–2257 (online), DOI: 10.1109/TCAD.2005.860952 (2006).

[72] Fang, E.J.W., Shih, T.C.-J. and Huang, D.S.-Y.: IR to routing challenge and solution for interposer-based design, *Proc. Asia South Pacific Des. Autom. Conf.*, pp.226–230 (online), DOI: 10.1109/ASPDAC.2015.7059009 (2015).

[73] Liu, W.-H., Chien, T.-K. and Wang, T.-C.: Metal Layer Planning for Silicon Interposers with Consideration of Routability and Manufacturing Cost, *Proc. Des. Autom. Test Europe*, pp.359:1–359:6 (online), DOI: 10.7873/DATE.2014.372 (2014).

[74] Wu, S.-T., Chien, H.-C., Lau, J.H., et al.: Thermal and mechanical design and analysis of 3D IC interposer with double-sided active chips, *Proc. Elec. Compon. Technol. Conf.*, pp.1471–1479 (online), DOI: 10.1109/ECTC.2013.6575766 (2013).

[75] Heinig, A. and Fischbach, R.: Enabling automatic system design optimization through Assembly Design Kits, *Proc. 3D Sys. Integ. Conf.*, pp.TS8.31.1–TS8.31.5 (online), DOI: 10.1109/3DIC.2015.7334602 (2015).

[76] Hosseini, S., Haas, M., Plettemeier, D., et al.: Integrated Optical Devices for 3D Photonic Transceivers, *3D Stacked Chips – From Emerging Processes to Heterogeneous Systems*, Elfadel, I.A.M. and Fettweis, G. (Eds.), chapter 13, Springer (online), DOI: 10.1007/978-3-319-20481-9 (2016).

[77] Ocak, I.E., Cheam, D.D., Fernando, S.N., et al.: A monolithic 9 degree of freedom (DOF) capacitive inertial MEMS platform, *Proc. Int. Elec. Devices Meeting*, pp.22.6.1–22.6.4 (online), DOI: 10.1109/IEDM.2014.7047103 (2014).

[78] Nesro, M.S., Sun, L. and Elfadel, I.M.: Compact modeling of microbatteries using behavioral linearization and model-order reduction, *Proc. Asia South Pacific Des. Autom. Conf.*, pp.713–718 (online), DOI: 10.1109/ASPDAC.2015.7059094 (2015).

[79] Takemoto, Y., Kato, H., Kondo, T., et al.: An efficient method to evaluate 4 million micro-bump interconnection resistances for 3D stacked 16-mpixel image sensor, *Proc. Int. Conf. Microelec. Test Struct.*, pp.2–5 (online), DOI: 10.1109/ICMTS.2016.7476162 (2016).

[80] Tang, H.Y., Lu, Y., Jiang, X., et al.: 3-D Ultrasonic Fingerprint Sensor-on-a-Chip, *J. Solid-State Circ.*, Vol.51, No.11, pp.2522–2533 (online), DOI: 10.1109/JSSC.2016.2604291 (2016).

[81] Killge, S., Neumann, N., Plettemeier, D., et al.: Optical Through-Silicon Vias, *3D Stacked Chips – From Emerging Processes to Heterogeneous Systems*, Elfadel, I.A.M. and Fettweis, G. (Eds.), chapter 12, Springer (online), DOI: 10.1007/978-3-319-20481-9 (2016).

[82] Odeh, M., Voort, B., Anjum, A., et al.: Gradient-index optofluidic waveguide in polydimethylsiloxane, *Applied Optics*, Vol.56, No.4, pp.1202–1206 (online), DOI: AO.56.001202 (2017).

[83] Cederström, L.: EDA Environments for 3D Chip Stacks, *3D Stacked Chips – From Emerging Processes to Heterogeneous Systems*, Elfadel, I.A.M. and Fettweis, G. (Eds.), chapter 9, Springer (online), DOI: 10.1007/978-3-319-20481-9 (2016).

[84] Shaeffer, D.K.: MEMS inertial sensors: A tutorial overview, *IEEE Communications Magazine*, Vol.51, No.4, pp.100–109 (online), DOI: 10.1109/MCOM.2013.6495768 (2013).

[85] Tsai, J.M., Daneman, M., Boser, B., et al.: Versatile CMOS-MEMS integrated piezoelectric platform, *Proc. Int. Conf. Solid-State Sens. Act. Microsys.*, pp.2248–2251 (online), DOI: 10.1109/TRANSDUCERS.2015.7181409 (2015).

[86] Horsley, D.A., Lu, Y., Tang, H.Y., et al.: Ultrasonic fingerprint sensor based on a PMUT array bonded to CMOS circuitry, *Proc. Int. Ultrason. Symp.*, pp.1–4 (online), DOI: 10.1109/ULTSYM.2016.7728817 (2016).

[87] Wang, N., Siow, L.Y., Ji, H., et al.: AlN Wideband Energy Harvesters with Wafer-Level Vacuum Packaging Utilizing Three-Wafer Bonding, *Proc. Int. Conf. Micro Elec. Mech. Sys.*, (online), DOI: 10.1109/MEMSYS.2017.7863539 (2017).

[88] Coventor Inc.: MEMS+IC Co-simulation in Cadence Viruoso, (online), available from ⟨http://www.coventor.com/mems-solutions/products/mems/mems-for-cadence⟩ (2016).

[89] Orcutt, J.S., Gill, D.M., Proesel, J., et al.: Monolithic silicon photonics at 25 Gb/s, *Proc. Opt. Fiber Comm. Conf. Exhib.*, pp.1–3 (online), DOI: 10.1364/OFC.2016.Th4H.1 (2016).

[90] Boeuf, F. and Ouellette, K.: Industrialization of Si-Photonics into a 300mm CMOS fab, *Proc. Int. Symp. VLSI Tech. Sys. App.*, pp.1–2 (online), DOI: 10.1109/VLSI-TSA.2016.7480504 (2016).

[91] Lim, A.E.J., Song, J., Fang, Q., et al.: Review of Silicon Photonics Foundry Efforts, *J. Sel. Topics Quantum Electr.*, Vol.20, No.4, pp.405–416 (online), DOI: 10.1109/JSTQE.2013.2293274 (2014).

[92] Denoyer, G., Cole, C., Santipo, A., et al.: Hybrid Silicon Photonic Circuits and Transceiver for 50 Gb/s NRZ Transmission Over Single-Mode Fiber, *J. Lightwave Technol.*, Vol.33, No.6, pp.1247–1254 (online), available from ⟨http://jlt.osa.org/abstract.cfm?URI=jlt-33-6-1247⟩ (2015).

[93] Xing, P. and Viegas, J.: Athermal Photonic Circuits for Optical On-Chip Interconnects, *3D Stacked Chips – From Emerging Processes to Heterogeneous Systems*, Elfadel, I.A.M. and Fettweis, G. (Eds.), chapter 15, Springer (online), DOI: 10.1007/978-3-319-20481-9 (2016).

[94] Cadence Inc.: Integrated electronics/photonic design automation environment, (online), available from ⟨https://www.cadence.com/content/cadence-www/global/en_US/home/solutions/photonics.html⟩ (2016).

[95] Chang, H.H., Hsiao, Z.C., Wang, J.C., et al.: Process integration and 3D chip stacking for low cost backside illuminated CMOS image sensor, *Proc. Int. Symp. VLSI Tech. Sys. App.*, pp.1–2 (online), DOI: 10.1109/VLSI-TSA.2015.7117587 (2015).

[96] Pham, N.P., Tutunjyan, N., Volkaerts, D., et al.: 3D integration technology using W2W direct bonding and TSV for CMOS based image sensors, pp.1–5 (online), DOI: 10.1109/EPTC.2015.7412378 (2015).

[97] Yole Développement: 3D IC and 2,5D TSV Interconnect for Advanced Packaging: From Technologies to Market, (online), available from ⟨http://www.yole.fr/iso_upload/News/2014/PR_3DICBusinessUpdate_YOLE_July2014.pdf⟩ (2014).

[98] IEEE: IEEE Standard for Test Access Port and Boundary-Scan Architecture, *IEEE Std 1149.1-2013* (*Revision of IEEE Std 1149.1-2001*), pp.1–444 (online), DOI: 10.1109/IEEESTD.2013.6515989 (2013).

[99] IEEE: IEEE Standard Testability Method for Embedded Core-based Integrated Circuits, *IEEE Std 1500-2005*, pp.1–136 (online), DOI: 10.1109/IEEESTD.2005.96465 (2005).

[100] Lee, H.-H.S. and Chakrabarty, K.: Test Challenges for 3D Integrated Circuits, *J. Des. Test*, Vol.26, No.5, pp.26–35 (online), DOI: 10.1109/MDT.2009.125 (2009).

[101] Wright, S.L., Polastre, R., Gan, H., et al.: Characterization of micro-bump C4 interconnects for Si-carrier SOP applications, *Proc. Elec. Compon. Technol. Conf.*, p.8 (online), DOI: 10.1109/ECTC.2006.1645716 (2006).

[102] Agrawal, M. and Chakrabarty, K.: Test-Cost Modeling and Optimal Test-Flow Selection of 3-D-Stacked ICs, *Trans. Comput.-Aided Des. Integr. Circuits Sys.*, Vol.34, No.9, pp.1523–1536 (online), DOI: 10.1109/TCAD.2015.2419227 (2015).

[103] Wang, R., Li, Z., Kannan, S., et al.: Pre-Bond Testing and Test-Path Design for the Silicon Interposer in 2.5D ICs, *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, Vol.PP, No.99, pp.1–11 (online), DOI: 10.1109/TCAD.2016.2629422 (2017).

[104] Lu, H., Lin, C. and Hung, W.: Interposer testing using dummy connections, Taiwan Semiconductor Manufacturing Company, Ltd., (online), available from ⟨https://www.google.com/patents/US8664540⟩ (2014).

[105] Chien, J.-H., Hsu, R.-S., Lin, H.-J., et al.: Contactless Stacked-die Testing for Pre-bond Interposers, *Proc. Des. Autom. Conf.*, pp.8:1–8:6 (online), DOI: 10.1145/2593069.2593111 (2014).

[106] Huang, L.R., Huang, S.Y., Sunter, S., et al.: Oscillation-Based Prebond TSV Test, *Trans. Comput.-Aided Des. Integr. Circuits Sys.*, Vol.32, No.9, pp.1440–1444 (online), DOI: 10.1109/TCAD.2013.2259626 (2013).

[107] Wang, R., Deutsch, S., Agrawal, M., et al.: The Hype, Myths, and Realities of Testing 3D Integrated Circuits, *Proc. Int. Conf. Comp.-Aided Des.*, pp.58:1–58:8 (online), DOI: 10.1145/2966986.2980097 (2016).

[108] Deutsch, S. and Chakrabarty, K.: Contactless pre-bond TSV fault diagnosis using duty-cycle detectors and ring oscillators, *Proc. Int. Test Conf.*, pp.1–10 (online), DOI: 10.1109/TEST.2015.7342389 (2015).

[109] Moore, B., Sellathamby, C., Cauvet, P., et al.: High throughput noncontact SiP testing, *Proc. Int. Test Conf.*, pp.1–10 (online), DOI: 10.1109/TEST.2007.4437595 (2007).

[110] Kim, J.S., Oh, C.S., Lee, H., et al.: A 1.2V 12.8GB/s 2Gb mobile Wide-I/O DRAM with 4x128 I/Os using TSV-based stacking, *Proc. Int. Solid-State Circ. Conf.*, pp.496–498 (online), DOI: 10.1109/ISSCC.2011.5746413 (2011).

[111] Marinissen, E.J.: Challenges and Emerging Solutions in Testing TSV-based 2 1/2D- and 3D-stacked ICs, *Proc. Des. Autom. Test Europe*, pp.1277–1282 (online), DOI: 10.1109/DATE.2012.6176689 (2012).

[112] Marinissen, E.J., Vermeulen, B., Hollmann, H., et al.: Minimizing pattern count for interconnect test under a ground bounce constraint, *J. Des. Test*, Vol.20, No.2, pp.8–18 (online), DOI: 10.1109/MDT.2003.1188257 (2003).

[113] Aung, M.T.L., Yoshikawa, T., Tan, C.S., et al.: Yield Enhancement of Face-to-Face Cu–Cu Bonding With Dual-Mode Transceivers in 3DICs, *Trans. VLSI Syst.*, Vol.25, No.3, pp.1023–1031 (online), DOI: 10.1109/TVLSI.2016.2623659 (2017).

[114] Marinissen, E.J., McLaurin, T. and Jiao, H.: IEEE Std P1838: DfT Standard-under-Development for 2.5D-, 3D-, and 5.5D-SICs, *Proc. Europe Test. Symp.*, pp.1–10 (online), DOI: 10.1109/ETS.2016.7519330 (2016).

[115] Saeed, S.M. and Sinanoglu, O.: A Comprehensive Design-for-Test Infrastructure in the Context of Security-Critical Applications, *J. Des. Test*, Vol.34, No.1, pp.57–64 (online), DOI: 10.1109/MDAT.2016.2527708 (2017).

[116] Subramanyan, P., Tsiskaridze, N., Li, W., et al.: Reverse Engineering Digital Circuits Using Structural and Functional Analyses, *Trans. Emerg. Top. Comp.*, Vol.2, No.1, pp.63–80 (online), DOI: 10.1109/TETC.2013.2294918 (2014).

[117] Wu, T.F., Ganesan, K., Hu, Y.A., et al.: TPAD: Hardware Trojan Prevention and Detection for Trusted Integrated Circuits, *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, Vol.35, No.4, pp.521–534 (online), DOI: 10.1109/TCAD.2015.2474373 (2016).

[118] Meade, T., Zhang, S. and Jin, Y.: IP protection through gate-level netlist security enhancement, *Integration, the VLSI Journal*, Vol.PP, No.99, pp.1–8 (online), DOI: 10.1016/j.vlsi.2016.10.014 (2016).

[119] Fern, N., San, I. and Cheng, K.-T.T.: Detecting Hardware Trojans in Unspecified Functionality Through Solving Satisfiability Problems, *Proc. Asia South Pac. Des. Autom. Conf.*, pp.598–604 (online), DOI: 10.1109/ASPDAC.2017.7858389 (2017).

[120] Bryant, R.E., Cheng, K.-T., Kahng, A.B., et al.: Limitations and challenges of computer-aided design technology for CMOS VLSI, *Proc. IEEE*, Vol.89, No.3, pp.341–365 (online), DOI: 10.1109/5.915378 (2001).

[121] Wang, L.C.: Experience of Data Analytics in EDA and Test - Principles, Promises, and Challenges, *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, Vol.PP, No.99, pp.1–1 (online), DOI: 10.1109/TCAD.2016.2621883 (2017).

[122] Wood, L.: Research and Markets: Outsourced Semiconductor Assembly and Test Market (OSAT) Trends, (online), available from ⟨http://www.businesswire.com/news/home/20140324005628/en/⟩ (2014).

[123] Roy, J.A., Koushanfar, F. and Markov, I.L.: Ending Piracy of Integrated Circuits, *Computer*, Vol.43, No.10, pp.30–38 (online), DOI: 10.1109/MC.2010.284 (2010).

[124] McCants, C.: Trusted Integrated Chips (TIC), Technical report, Intelligence Advanced Research Projects Activity (IARPA) (online), available from ⟨https://www.iarpa.gov/index.php/research-programs/tic⟩ (2011).

[125] Rajendran, J., Sinanoglu, O. and Karri, R.: Regaining Trust in VLSI Design: Design-for-Trust Techniques, *Proc. IEEE*, Vol.102, No.8, pp.1266–1282 (online), DOI: 10.1109/JPROC.2014.2332154 (2014).

[126] Rajendran, J.J., Sinanoglu, O. and Karri, R.: Building Trustworthy Systems Using Untrusted Components: A High-Level Synthesis Approach, *Trans. VLSI Syst.*, Vol.24, No.9, pp.2946–2959 (online), DOI: 10.1109/TVLSI.2016.2530092 (2016).

[127] Yang, K., Hicks, M., Dong, Q., et al.: A2: Analog Malicious Hardware, *Proc. Symp. Sec. Priv.*, pp.18–37 (online), DOI: 10.1109/SP.2016.10 (2016).

[128] Mishra, P., Bhunia, S. and Tehranipoor, M. (Eds.): *Hardware IP Security and Trust*, Springer (online), DOI: 10.1007/978-3-319-49025-0 (2017).

[129] Valamehr, J., Tiwari, M., Sherwood, T., et al.: Hardware Assistance for Trustworthy Systems Through 3-D Integration, *Proc. Ann. Comp. Sec. App. Conf.*, pp.199–210 (online), DOI: 10.1145/1920261.1920292 (2010).

[130] Valamehr, J., Sherwood, T., Kastner, R., 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 (online), DOI: 10.1109/TCAD.2012.2227257 (2013).

[131] Cioranesco, J.M., Danger, J.L., Graba, T., et al.: Cryptographically secure shields, *Proc. Int. Symp. Hardw.-Orient. Sec. Trust*, pp.25–31 (online), DOI: 10.1109/HST.2014.6855563 (2014).

[132] Bao, C. and Srivastava, A.: 3D Integration: New opportunities in defense against cache-timing side-channel attacks, *Proc. Int. Conf. Comp. Des.*, pp.273–280 (online), DOI: 10.1109/ICCD.2015.7357114 (2015).

[133] Sepúlveda, J., Gogniat, G., Flórez, D., et al.: TSV protection: Towards secure 3D-MPSoC, *Proc. Latin Amer. Symp. Circ. Sys.*, pp.1–4 (online), DOI: 10.1109/LASCAS.2015.7250419 (2015).

[134] Xie, Y., Bao, C., Serafy, C., et al.: Security and Vulnerability Implications of 3D ICs, *Trans. Multi-Scale Comp. Sys.*, Vol.2, No.2, pp.108–122 (online), DOI: 10.1109/TMSCS.2016.2550460 (2016).

[135] Gu, P., Li, S., Stow, D., et al.: Leveraging 3D Technolo-

gies for Hardware Security: Opportunities and Challenges, *Proc. Great Lakes Symp. VLSI*, pp.347–352 (online), DOI: 10.1145/2902961.2903512 (2016).

[136] Dofe, J., Yu, Q., Wang, H., et al.: Hardware Security Threats and Potential Countermeasures in Emerging 3D ICs, *Proc. Great Lakes Symp. VLSI*, pp.69–74 (online), DOI: 10.1145/2902961.2903014 (2016).

[137] Dofe, J., Yan, C., Kontak, S., et al.: Transistor-Level Camouflaged Logic Locking Method for Monolithic 3D IC Security, *Proc. Asian Hardw.-Orient. Sec. Trust Symp.*, pp.1–6 (online), DOI: 10.1109/AsianHOST.2016.7835570 (2016).

[138] Knechtel, J. and Sinanoglu, O.: On Mitigation of Side-Channel Attacks in 3D ICs: Decorrelating Thermal Patterns from Power and Activity, *Proc. Des. Autom. Conf.*, pp.1–6 (online), DOI: 10.1145/3061639.3062293 (2017).

[139] Mysore, S., Agrawal, B., Srivastava, N., et al.: Introspective 3D chips, *SIGOPS Operat. Sys. Rev.*, Vol.40, No.5, pp.264–273 (online), DOI: 10.1145/1168857.1168890 (2006).

[140] Tezzaron Semiconductor: 3D-ICs and Integrated Circuit Security, Technical report, Tezzaron Semiconductor (online), available from ⟨http://tezzaron.com/media/3D-ICs_and_Integrated_Circuit_Security.pdf⟩ (2008).

[141] Peng, Y., Petranovic, D. and Lim, S.K.: Multi-TSV and E-Field Sharing Aware Full-chip Extraction and Mitigation of TSV-to-Wire Coupling, *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, Vol.34, No.12, pp.1964–1976 (online), DOI: 10.1109/TCAD.2015.2446934 (2015).

[142] Rack, M., Raskin, J.P., Sun, X., et al.: Fast and Accurate Modelling of Large TSV Arrays in 3D-ICs Using a 3D Circuit Model Validated Against Full-Wave FEM Simulations and RF Measurements, *Proc. Elec. Compon. Tech. Conf.*, pp.966–971 (online), DOI: 10.1109/ECTC.2016.227 (2016).

[143] Rosenfeld, K. and Karri, R.: Security-aware SoC test access mechanisms, *VLSI Test Symp.*, pp.100–104 (online), DOI: 10.1109/VTS.2011.5783765 (2011).

[144] van der Veen, V., Fratantonio, Y., Lindorfer, M., et al.: Drammer: Deterministic Rowhammer Attacks on Mobile Platforms, *Proc. Comp. Comm. Sec.*, pp.1675–1689 (online), DOI: 10.1145/2976749.2978406 (2016).

[145] Xiao, K., Forte, D., Jin, Y., et al.: Hardware Trojans: Lessons Learned After One Decade of Research, *Trans. Des. Autom. Elec. Sys.*, Vol.22, No.1, pp.6:1–6:23 (online), DOI: 10.1145/2906147 (2016).

[146] Hutter, M. and Schmidt, J.-M.: The Temperature Side Channel and Heating Fault Attacks, *Smart Card Research and Advanced Applications*, *Lect. Notes Comp. Sci.*, Vol.8419, Springer, pp.219–235 (online), DOI: 10.1007/978-3-319-08302-5_15 (2014).

[147] Masti, R.J., Rai, D., Ranganathan, A., et al.: Thermal Covert Channels on Multi-core Platforms, *Proc. USENIX Sec. Symp.*, pp.865–880 (online), available from ⟨https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/masti⟩ (2015).

[148] Kim, L.W. and Villasenor, J.D.: A System-On-Chip Bus Architecture for Thwarting Integrated Circuit Trojan Horses, *Trans. VLSI Syst.*, Vol.19, No.10, pp.1921–1926 (online), DOI: 10.1109/TVLSI.2010.2060375 (2011).

[149] Bhunia, S., Abramovici, M., Agrawal, D., et al.: Protection Against Hardware Trojan Attacks: Towards a Comprehensive Solution, *J. Des. Test*, Vol.30, No.3, pp.6–17 (online), DOI: 10.1109/MDT.2012.2196252 (2013).

[150] Sepúlveda, J., Flórez, D. and Gogniat, G.: Reconfigurable security architecture for disrupted protection zones in NoC-based MPSoCs, *Proc. ReCoSoc*, pp.1–8 (online), DOI: 10.1109/ReCoSoC.2015.7238098 (2015).

[151] Chandrasekharan, A., Schmitz, K., Kuhne, U., et al.: Ensuring safety and reliability of IP-based system design – A container approach, *Proc. Int. Symp. Rapid System Prototyping*, pp.76–82 (online), DOI: 10.1109/RSP.2015.7416550 (2015).

[152] Chen, X., Wang, L., Wang, Y., et al.: A General Framework for Hardware Trojan Detection in Digital Circuits by Statistical Learning Algorithms, *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, Vol.PP, No.99, p.1 (online), DOI: 10.1109/TCAD.2016.2638442 (2017).

[153] Wei, X., Diao, Y. and Wu, Y.L.: To Detect, Locate, and Mask Hardware Trojans in digital circuits by reverse engineering and functional ECO, *Proc. Asia South Pac. Des. Autom. Conf.*, pp.623–630 (online), DOI: 10.1109/ASPDAC.2016.7428081 (2016).

[154] Hasan, S.R., Mossa, S.F., Elkeelany, O.S.A., et al.: Tenacious hardware trojans due to high temperature in middle tiers of 3-D ICs, *Proc. Midwest Symp. Circ. Sys.*, pp.1–4 (online), DOI: 10.1109/MWSCAS.2015.7282148 (2015).

[155] Imeson, F., Emtenan, A., Garg, S., et al.: Securing Computer Hardware Using 3D Integrated Circuit (IC) Technology and Split Manufacturing for Obfuscation, *Proc. USENIX Sec. Symp.*, pp.495–510 (online), available from ⟨https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_imeson.pdf⟩ (2013).

[156] Rajendran, J., Sinanoglu, O. and Karri, R.: Is split manufacturing secure?, *Proc. Des. Autom. Test Europe*, pp.1259–1264 (online), DOI: 10.7873/DATE.2013.261 (2013).

[157] Xiao, K., Forte, D. and Tehranipoor, M.M.: Efficient and secure split manufacturing via obfuscated built-in self-authentication, *Proc. Int. Symp. Hardw.-Orient. Sec. Trust*, pp.14–19 (online), DOI: 10.1109/HST.2015.7140229 (2015).

[158] Xie, Y., Bao, C. and Srivastava, A.: Security-Aware Design Flow for 2.5D IC Technology, *Proc. Int. Worksh. Trustw. Emb. Dev.*, pp.31–38 (online), DOI: 10.1145/2808414.2808420 (2015).

[159] Yang, P.-L. and Marek-Sadowska, M.: Making Split-fabrication More Secure, *Proc. Int. Conf. Comp.-Aided Des.*, pp.91:1–91:8 (online), DOI: 10.1145/2966986.2967053 (2016).

[160] Wang, Y., Chen, P., Hu, J., et al.: The Cat and Mouse in Split Manufacturing, *Proc. Des. Autom. Conf.*, pp.165:1–165:6 (online), DOI: 10.1145/2897937.2898104 (2016).

[161] Magaña, J., Shi, D. and Davoodi, A.: Are Proximity Attacks a Threat to the Security of Split Manufacturing of Integrated Circuits?, *Proc. Int. Conf. Comp.-Aided Des.*, pp.90:1–90:7 (online), DOI: 10.1145/2966986.2967006 (2016).

[162] DeVale, J., Rakvic, R. and Rudd, K.: Another dimension in integrated circuit trust, *J. Cryptogr. Eng.*, pp.1–12 (online), DOI: 10.1007/s13389-017-0164-7 (2017).

Johann Knechtel received his M.Sc. in Information Systems Engineering (Dipl.-Ing.) in 2010 and Ph.D. in Computer Engineering (Dr.-Ing.) in 2014, both from TU Dresden, Germany. He is a Postdoctoral Associate with the Design for Excellence Lab, in the Department of Electrical and Computer Engineering, at the New York University Abu Dhabi (NYUAD), UAE. Dr. Knechtel was a Postdoctoral Researcher in 2015–2016 at the Masdar Institute of Science and Technology, Abu Dhabi. From 2010 to 2014, he was a Research Associate and Scholar with the DFG Graduate School on "Nano- and Biotechnologies for Packaging of Electronic Systems" and the Institute of Electromechanical and Electronic Design, both hosted at the TU Dresden. In 2012, he was a Research Assistant with the Department of Computer Science and Engineering, Chinese University of Hong Kong, China. In 2010, he was a Visiting Research Student with the Department of Electrical Engineering and Computer Science, University of Michigan, USA. His research interests cover VLSI Physical Design Automation, with particular focus on 3D Integration and Hardware Security. In addition to various conference papers, he has authored 8 journal papers, invited papers and book chapters on these topics. Dr. Knechtel is an active member of the community, serving as reviewer for Elsevier Integration, the VLSI journal, IEEE Transactions on Computers (TC), IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), ACM Transactions on Design Automation of Electronic Systems (TODAES), IEEE Transactions on Very Large Scale Integration Systems (TVLSI), as well as for various conferences: ASPDAC, DAC, DATE, GLSVLSI, ICCAD, ISPD, MWSCAS, SLIP, and IOLTS. He is a member of IEEE and ACM.

Ozgur Sinanoglu is an Associate Professor of Electrical and Computer Engineering at New York University Abu Dhabi. He earned his B.S. degrees, one in Electrical and Electronics Engineering and one in Computer Engineering, both from Bogazici University, Turkey in 1999. He obtained his M.S. and Ph.D. in Computer Science and Engineering from University of California San Diego in 2001 and 2004, respectively. He has industry experience at TI, IBM and Qualcomm, and has been with NYU Abu Dhabi since 2010. During his Ph.D., he won the IBM Ph.D. Fellowship Award twice. He is also the recipient of the Best Paper Awards at IEEE VLSI Test Symposium 2011 and ACM Conference on Computer and Communication Security 2013. Professor Sinanoglu's research interests include design-for-test, design-for-security and design-for-trust for VLSI circuits, where he has around 160 conference and journal papers, and 20 issued and pending US Patents. Sinanoglu has given more than a dozen tutorials on hardware security and trust in leading CAD and test conferences, such as DAC, DATE, ITC, VTS, ETS, ICCD, ISQED, etc. He is serving as track/topic chair or technical program committee member in about 15 conferences, and as (guest) associate editor for IEEE TIFS, IEEE TCAD, ACM JETC, IEEE TETC, Elsevier MEJ, JETTA, and IET CDT journals. Professor Sinanoglu is the director of the Design-for-Excellence Lab at NYU Abu Dhabi. His recent research in hardware security and trust is being funded by US National Science Foundation, US Department of Defense, Semiconductor Research Corporation, and Mubadala Technology.

Ibrahim (Abe) M. Elfadel is a Professor of Electrical and Computer Engineering at the Masdar Institute, Khalifa University of Science and Technology, Abu Dhabi, UAE. Since May 2013, he has been the founding co-director of the Abu Dhabi Center of Excellence on Energy-Efficient Electronic Systems (ACE^{4}S), and since May 2014, he has been the Program Manager of TwinLab MEMS, a joint collaboration with GLOBALFOUNDRIES and the Singapore Institute of Microelectronics on microelectromechanical systems. Between November 2012 and October 2015, he was the founding co-director of Mubadala's TwinLab 3DSC, a joint research center on 3D integrated circuits with the Technical University of Dresden, Germany. He also headed the Masdar Institute Center for Microsystems (iMicro) from November 2013 until March 2016. Between 1996 and 2010, he was with the corporate CAD organizations at IBM Research and the IBM Systems and Technology Group, Yorktown Heights, NY, where he was involved in the research, development, and deployment of CAD tools and methodologies for IBM's high-end microprocessors. In addition to 3D integrated circuits, his current research interests include integrated photonics; power and thermal management of multi-core processors; energy-efficient cloud computing; low-power, embedded digital-signal processing; energy-efficient IoT communications; and modeling and integration of micro power sources. He is currently leading Design Enablement at the Masdar Institute Center of Excellence on Integrated Photonics (CEIPh) in collaboration with the Semiconductor Research Corporation and GLOBALFOUNDRIES. Dr. Elfadel is the recipient of six Invention Achievement Awards, one Outstanding Technical Achievement Award and one Research Division Award, all from IBM, for his contributions in the area of VLSI CAD. He is the inventor or co-inventor of 50 issued US patent. In 2014, he was the co-recipient of the D. O. Pederson Best Paper Award from the IEEE Transactions on Computer-Aided Design Automation for Integrated Circuits and Systems. He is also the co-editor (with Professor Gerhard Fettweis) of "3D Stacked Chips: From Emerging Processes to Heterogeneous Systems," Springer, 2016. Between 2009 and 2013, Dr. Elfadel served as an Associate Editor of the IEEE Transactions on Computer-Aided Design. He is currently serving as Associate Editor of the IEEE Transactions on VLSI Systems and on the Editorial Board of the Microelectronics Journal (Elsevier). Dr. Elfadel has also served on the Technical Program Committees of several top conferences, including DAC, ICCAD, ASPDAC, DATE, ICCD, ICECS, and MWSCAS. He will be the General Co-chair of the IFIP/IEEE 25th International Conference on Very Large Scale Integration (VLSI-SoC 2017), Abu Dhabi, UAE, October 23-25, 2017. He received his Ph.D. from MIT in 1993.

Jens Lienig received his M.Sc. (diploma), Ph.D. (Dr.-Ing.) and Habilitation degrees in Electrical Engineering from Dresden University of Technology, Dresden, Germany, in 1988, 1991 and 1996, respectively. He is currently a Full Professor of Electrical Engineering at Dresden University of Technology (TU Dresden) where he is also Director of the Institute of Electromechanical and Electronic Design (IFTE). From 1999 to 2002, he worked as Tool Manager at Robert Bosch GmbH in Reutlingen, Germany, and from 1996 to 1999, he was with Tanner Research Inc. in Pasadena, CA. From 1994 to 1996, he was a Visiting Assistant Professor with the Department of Computer Science, University of Virginia, Charlottesville, VA, and from 1991 to 1994, a Postdoctoral Fellow at Concordia University in Montréal, QC, Canada. His current research interests are in physical design automation, with a special emphasis on electromigration avoidance, 3D design, and constraint-driven design methodologies of analog circuits. Professor Lienig has served on the Technical Program Committees of the DATE, SLIP and ISPD conferences. He is a Senior Member of IEEE.

Cliff C. N. Sze is currently a software engineer at Google. Previously, he was a research staff member at the IBM T. J. Watson Research Center and the Austin Research Laboratory. Dr. Sze filed more than 90 patent applications and was granted over 50 patents. His research interests include the design and analysis of algorithms in order to solve a wide range of practical problems such as e-commerce, healthcare analytics, cancer radiation therapy, and electronic design automation. He received his bachelor and master degrees from the Department of Computer Science and Engineering at the Chinese University of Hong Kong, and his Ph.D. degree in computer engineering from the Department of Electrical Engineering at Texas A&M University. As the senior members of IEEE and ACM, Dr. Cliff Sze has been actively serving the academic/research community, for example, serving as the general chair and technical program committee chair of International Symposium on Physical Design, and being appointed as an associate editor for ACM Transactions on Design Automation of Electronic Systems (TODAES). He is a recipient of the ACM Special Interest Group on Design Automation (SIGDA) technical leadership award.

(Invited by Editor-in-Chief: *Masanori Hashimoto*)