

Chapter 19: Security

Executive Summary

Trends in semiconductors and their applications pose challenges to security and trustworthiness. On one hand, leading-edge processors are the “brains” behind critically-important systems and infrastructure, including networking and communications, electric power grids, finance, military and aerospace systems. On the other hand, smaller embedded processors, sensors and other electronic components provide “smart” functionality and connectivity in a variety of applications, such as automotive braking and airbag systems, personal healthcare, industrial controls, and the rapidly growing list of other connected devices often referred to as the Internet of Things. The wide range of devices and applications and the exponential growth in the number of connected “things” has made security and trustworthiness a prime concern.

Section 1. General Cybersecurity Hardware Challenges and Needs[1]

Cybersecurity threats can manifest themselves either through software or hardware. The majority of threats occur through software attacks, providing access from many sources such as email attachments, fake web sites, unsecure wireless, social networking or infected USB drives. These attacks typically use vulnerabilities in the software that facilitate unauthorized access to and control of the infected system. In other attacks, the communication interface is used to forge messages or software updates, inject protocol faults, spy on the messages, or use man-in-the-middle attacks to obtain valuable information. Mitigation strategies for these attacks usually entail the installation of software updates addressing these vulnerabilities. Simple avoidance of unknown or uncontrolled sources of software is the most effective prevention strategy, along with potential virus protection software. These software threats are generally not specific to the hardware and as such are outside the scope of the HI security roadmap. Hardware security threats, on the other hand, are impacted greatly by the design and integration of the hardware components of a chip and the way chips are integrated into a functional system or a subsystem at the package level, board level, and system level. These hardware attacks fall into seven broad classes: interface leakage, supply-channel attacks, side channel attacks, chip counterfeiting, physical tampering with the system, fault injection attacks, and reverse engineering attacks. Table 1 summarizes these hardware attack classes and typically employed mitigation strategies.

Table 1. Hardware Attack Classes

Hardware Attack Vector	Impact	Mitigation Strategy
Interface Leakage	Unauthorized access directly at interfaces or through test mechanisms/interfaces	Design for security, interface obfuscation
Supply Chain Attacks	Hidden/delayed unwanted functionality or security compromise (confidentiality, integrity, or availability), Trojans, etc.	Design validation, parasitic detection, active triggering at test or validation; IP/design/materials provenance
Side Channel Attacks	Passive access to secure information such as encryption keys through observation of system signatures such as power, EM or timing	Making designs side-channel resistant by analyzing side-channel leakage (timing-based, power-based, electromagnetic, acoustic, optical, thermal, etc.) through simulations and blocking leakage through design changes
Chip Counterfeiting	Unauthorized use of aged or production of duplicate or compromised chips	Secured chip odometers and unique authentication based on physical unclonable functions
Physical Tampering	Invasive/semi-invasive access to secure information including reverse engineering	Sensors which detect intrusion and deactivate system
Fault Injection Attacks	Control Flow/Data Integrity with the purpose of bypassing security implemented in a design	Fault-tolerant methods to be utilized to increase the robustness of execution and data integrity
Reverse Engineering Attacks	Inspection of hardware and firmware (including ROM code and micro-code) to determine the functional elements and their interactions, to get access to embedded secrets, to find vulnerabilities and weaknesses, and to launch other attacks such as fault attacks, physical attacks, and side channel attacks, or discover ways for physical tampering or chip counterfeiting	Tamper-proof fixtures and layout obfuscation such as blind/buried vias or logic locking.

Please note that taxonomies for classification of hardware attacks are under development. Figure 1 shows a taxonomy of physical attacks (TrustHub^[2]) with more details – from left to right: passive versus active; invasive, non-invasive, or semi-invasive; attack vectors, and actual attack types. While many of the attack vectors can be found in Table 1, the mapping to those in Figure 1 is not one-to-one.

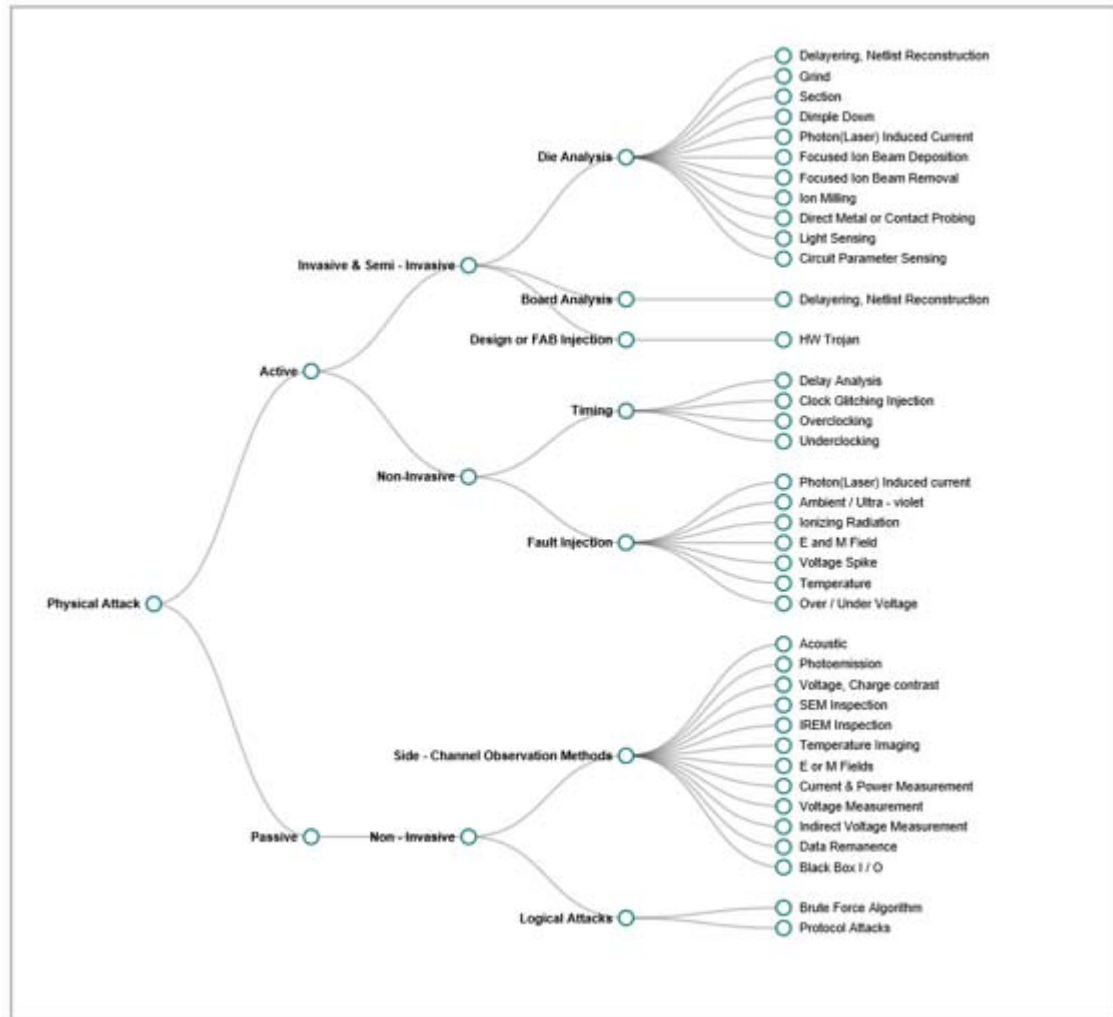


Figure 1. Taxonomy of physical attacks.[2]

Design and manufacture of today’s complex semiconductor circuits and systems require many steps and involve the work of hundreds of engineers, typically distributed across multiple locations and organizations worldwide. Moreover, today’s semiconductor chip is likely to include design modules or blocks (also referred to as intellectual-property, or IP, blocks) from multiple sources. Detailed specifications are converted into schematics (by mapping the specifications into different levels of abstraction: architectural, behavioral, micro-architectural, register transfer, transistor, and device), and then physical designs that may include billions of transistors. Many processes have been developed, and considerable resources are invested along the design and manufacturing path to verify, test and validate that the product performs as intended. However, to date, these processes do not provide 100% confidence about whether the chip has been altered such that it provides unauthorized access or control. Such undesirable behavior can be due to a weakness in the design that results in an unintentional side channel, or due to maliciously inserted functionality or “Trojan” hardware.

Attention to design for security and security validation has increased, and most large semiconductor design and manufacturing companies have included design for security and validation into their standard processes. The main focus is still to make sure that semiconductor circuits and systems are designed so as to make it feasible or easier to verify, manufacture and test during subsequent steps. What is needed is an understanding of design for security by all semiconductor design and manufacturing companies and paying utmost attention to it, with the objective of decreasing the likelihood of unintended behavior or access, increasing resistance and resilience to tampering and

counterfeiting, and improving the ability to provide authentication in the field. Design for security still requires new scalable solutions including strategies for architecture and specification, and tools for synthesis, physical design, test, and verification, especially at the stages of design in which formal methods are currently weak or absent. Methods and procedures targeting the early stages of design are likely to be more effective and affordable.

It is imperative to develop a theoretical basis for hardware security in order to design systems that are free of vulnerability and that are assured and resilient against attacks, even vulnerabilities and attacks that are not (yet) known. Ideally, such a mathematical model would abstract the environment of threats and responses and formalize precisely engineering concepts of system security, such as (response) closeness, safeness, vulnerability, attack, etc. Metrics to assess system security and quantify assurance could be developed from such a formal model. Existing and new automation and design tools may use the abstraction and metrics to specify security primitives as numeric attributes and allow trade-off with other design primitives of the system under design.

A successful design for security solution needs to be integrated with other design features and considerations, taking into account competing demands from system designers and manufacturers. For example, as system complexity grows, the demand for greater observability and controllability during manufacture and in the post-manufacturing and integration environments leads to increased risk of side channel attack. Designing capabilities that allow for on-line self-test, recovery, adaptation or reconfiguration also increases the risk of side channel attack. The risks associated with these design and manufacturing techniques need to be carefully studied and mitigated or neutralized. The role of multidisciplinary teams in mitigating these risks is of paramount importance.

Threats and challenges faced today by semiconductor security include, but are not limited to, those listed below:

- Unwanted functionality in specification, design or implementation at the behavioral, register-transfer level (RTL), logical or physical level. Unwanted functionality may be malicious or inadvertent. This includes incomplete and ambiguous specifications or implementations.
- Dependencies at interfaces that lead to leakage of sensitive information or weakness to attack. This includes time-dependent behavior or improper reliance of timeouts on external signals.
- Counterfeiting of semiconductor-based parts/products.
- Unauthorized access to sensitive data or control functions. This includes access to keys or sensitive internal data and controls.
- Maliciously inserted hardware Trojans and other forms of tampering with a design at any stage of the design cycle, including during manufacturing.
- Observation of signals of an electronic circuit while in operation, via a side channel.
- Tampering with an electronic circuit while in operation by fault injection.
- Identification of poor resistance to tampering, whether at a functional, logical or electrical level – in particular, resistance to known tampering methods, such as power, thermal or irradiation attacks.
- Hardware authentication and fingerprinting.
- Provenance of circuitry, including verification and tracking of IP blocks and of lack of tampering.
- Dependence on external components that could leak sensitive information or are not verifiable and hence vulnerable to attack.
- A formal and quantifiable specification of security and/or baselines that enable integrity checking at run time.

In the world of interconnected IoT devices, there is a growing need for focused research on design for security. Specifically, this requires research to develop designs, analysis strategies, processes and tools for secure, trustworthy, safe, reliable and privacy-preserving chips, as well as computing and communications systems. This research needs to target decreasing the likelihood of unintended behavior or access, increasing resistance and resilience to tampering, and improving the ability to provide authentication throughout the supply chain and in the field.

The following topics are representative of relevant research areas in the IoT security space:

- Architecture and design. Approaches, models and frameworks for reasoning about and specifying hardware-specific security properties. These design and architecture approaches should not be studied in isolation; the impact of security at the level of circuits and processors must be understood in terms of system-wide functionality, performance, and power goals.
- Principles, properties and metrics. Hardware security design principles and semiconductor-specific properties. Security metrics for evaluating or comparing designs, and that are extensible and potentially useful for privacy composition or for providing trust evidence at the system level.

- Verification. Tools, techniques, and methodologies for verifying hardware-specific security properties and enforcing security design principles. Innovative approaches to establish safety properties without knowing all aspects of the design, and thereby providing strong provable assurance. Approaches to increase automation of security verification and analysis.
- Embedded software and firmware. Assurance strategies and techniques to reduce vulnerabilities in embedded software and firmware, and for providing updates to address known vulnerabilities discovered after deployment in the field.
- Authentication and attestation. Models for the insertion of artifacts or design elements that are verifiable during design and throughout the life cycle. Supporting issues, such as the generation, protection and establishment of trust models for hardware-implemented keys, are also of interest.

Section 2. Specific HI Security Needs

Specific Heterogeneous Integration Cybersecurity Research Needs

The worlds of IC design, packaging design and design for security are converging with heterogeneous integration initiatives. Emerging technologies such as fan-out wafer-level packaging (FOWLP), silicon interposers, Wafer-On-Wafer (WoW), Package-On-Package (POP), 3D IC, 2.5D IC and Fan Out with Redistribution Layer (FO w RDL) require many IC and packaging suppliers to work together to optimize the security of the entire system, not just the individual elements. Design and verification for security presents unique challenges that traditional security tools and methodologies cannot solve. At a very high level, heterogeneous integration exacerbates three fundamental security risks: 1) it uses many diverse chips from a broad supply chain, 2) it puts these chips in much closer physical contact with shared resources which increases the threat of side channel attacks from a malicious chip, and 3) it increases the communication bandwidth, connectivity and vulnerabilities between these chips.

In particular, the increased number of potential attack surfaces for HI can initially be viewed negatively, but appropriate design insights can substantially improve the system security. Concepts such as split manufacturing between the various system components, enhanced side channel attack countermeasures, improved authentication, hierarchical security architectures and system level design tools can significantly improve security. By bringing together design houses, OSATs, foundries, OEMs and EDA vendors with security tools that can operate in both the IC and packaging domains, advanced HI systems can significantly reduce their inherent security vulnerabilities.

Many aspects of heterogeneous integration have potentially profound impact on system security. Since the scope of HI is so broad, it is not possible to discuss all these impacts in detail. Table 2 attempts to briefly characterize these impacts based on their association with each of the other HIR TWGs.

Table 2: First order security impacts of HIR TWG

Associated HIR TWG	First Order Security Impacts
Single Chip and Multi Chip Packaging	Additional interface, information flow and authentication and confidentiality concerns
Integrated Photonics	Side-channel attacks (SCA) of optical fibers requires closer proximity than that for EM SCA
Integrated Power Devices	DP SCA at a more local scale is more difficult but potentially higher in information content
MEMS and Sensor Integration	Local sensor integration can better hinder tampering and reverse engineering
RF and Analog Mixed Signal	Major impacts with wireless communication and wireless updates
Materials and Emerging Research Materials	Integration of magnetic materials can better shield EM signals
Emerging Research Devices	Qubits and entangled communications can set new security paradigms, spin based devices have additional degree of entropy
Interconnect	Major effects on chip interconnectivity and vulnerabilities (see below)
Test	Flexible test methodologies without secure design exacerbate vulnerabilities (see below)
Supply Chain	Multiple suppliers for multiple chips necessitate new interface controls (see below)
SiP	Increased proximity and connectivity of chips from diverse suppliers presents increased risks
3D + 2.5D	Major effects on chip proximity and vulnerability to SCA (see below)
WLP	Increased proximity and connectivity of chips from diverse suppliers presents increased risks
Mobile	Wireless communication for system updates increases risks
IoT	Increased connectivity of chips from diverse suppliers presents increased risks
Medical and Health	Life-threatening risks need increased security partitioning and safe mode defaults (see below)
Automotive	Life-threatening risks need increased security partitioning and safe mode defaults (see below)
High Performance Computing & Data	High inter-chip bandwidth poses unique security screening challenges
Aerospace and Defense	Life-threatening risks need increased security partitioning and safe mode defaults (see below)
Co-Design and Simulation	System design for security is becoming an imperative

Interconnect

Heterogeneous integration is primarily driven by the need to integrate a greater amount of diverse functionality into a smaller form factor – be it mobile phones, watches, or medical devices. To first order, this compaction has the immediate advantage of decreasing the lengths of interconnects with the related scaling reduction of both power and latency. There is also a general increase in the number of associated chips with needs for secure interfaces between them. The additional drive towards increased interconnect density has enabled increased bandwidth connectivity between the different chips in the system. Several HI process options such as WLP also provide for additional fan-out redistribution layers.

From a security perspective, most of these changes have negative consequences. An increase in the number of chip interfaces and the increase in the bandwidth between the chips provides both a greater number and richer content of attack surfaces. The closer proximity of chips to each other and a potentially higher bandwidth connectivity between them increases the risk of side channel attacks. The only security benefits of HI interconnect scaling are associated with the smaller Electro-Magnetic (EM) and differential power signatures of shorter interconnect lines and the finer scale and closer proximity probing required to extract EM signatures.

Test

Enabling a large number of diverse chips from many different suppliers to be both flexibly and effectively tested presents a major security challenge if appropriate design-for-test and simultaneous design-for-security algorithms are not employed. Scan chains used in test are often used as one the most effective attack surfaces. HI test will require substantial partitioning and control modifications to minimize these risks. This is particularly important when shared resources cannot be effectively partitioned at test.

Supply Chain

Heterogeneous implies both diverse functionality and diverse component suppliers. Both of these changes generate intrinsic challenges to system security. This diverse functionality necessitates greater flexibility and security exposure at interfaces, especially as it relates to testing of a diverse set of functions. Clearly an increase in the number of different and diverse component suppliers not only increases the potential number of malicious chips but also drives the need for implementing security-based standardization at these interfaces to reduce these risks. Establishing standards for these interfaces is one of the principal challenges to the future of highly dependable products based on HI.

2.5D and 3D

To first order, both 2.5D and 3D processing are just an extension of the general trends of HI interconnect evolution, placing chips in closer proximity with greater inter-chip bandwidth. However, both 2.5D and 3D, and several other vertical integration approaches, have a fundamental geometrical change of placing die in direct contact with each other. This has both potential advantages and disadvantages for system security.

The direct contact between dies greatly increases the risk of side channel attacks from a malicious chip in the stack. In particular, a spy chip inserted in the stack has orders of magnitude increase in sensitivity and spatial resolution in extracting EM, thermal and power signatures from the chips immediately above and below it. This threat must be addressed with both design and shielding mitigation strategies. Security advantages of the vertical stack include that an appropriately vertically inserted system security control chip which can provide more effective isolation than more-distributed 2D geometries, and thus external SCA signatures are typically reduced.

Applications with Life-Threatening Risks

Several HI applications such as medical, automotive, aerospace and defense have potentially life-threatening consequences for security breaches. For these particular applications, there are much more restrictive requirements for security and high dependability. In particular, system monitoring, dynamic response and partitioning for security attack mitigation is essential. In addition, the system must be fundamentally designed for high dependability so that it will always be able to operate in a safe state. Such design requirements go beyond simply security threats, but these threats must receive particular attention due to their dynamic and unpredictable nature.

Co-design

As referenced multiple times above, the proposed solution to the majority of the HI security problems is stated simply as design for security. The real challenge for HI security is that there is currently no coherent design-for-security approach which addresses the specific HI security risks described above. In particular, HI requires a new system-level design paradigm which extends across multiple chips and manufacturers. The EDA community is just starting to develop system design tools that address some of the unique HI needs, but currently they focus on functionality and performance with little attention to security. As described in the split manufacturing section below, there are clearly tremendous security benefits that can be achieved by such a system-level design-for-security approach.

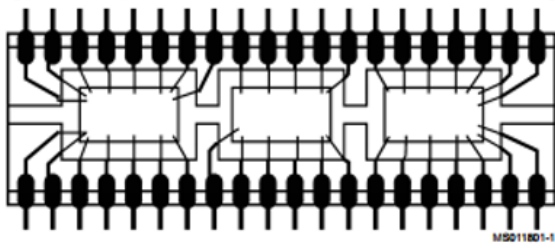
Section 3. Specific HI Security Opportunities

A. Information Flow and Authentication

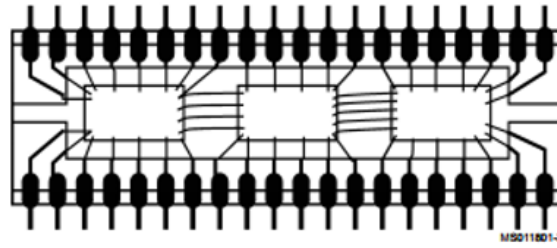
This section summarizes the techniques that can be employed to improve the security of integrated heterogeneous systems encapsulated in a package. Subsection 1 introduces several common package types used in industry for Heterogeneous Integrated (HI) Systems. Subsections 2 and 3 described techniques to secure information flow for HI systems, and Subsection 4 goes over several techniques for authentication of the packaged IC's, which are important from the supply-chain security perspective.

1. Multiple Chip Package Types

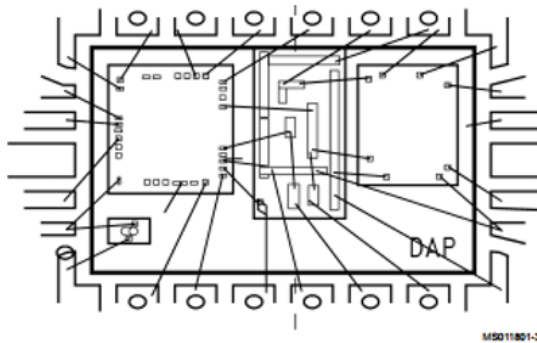
Integrated circuits (IC's) today may use multiple dies in a package, as it gives more flexibility to design a more complex system (or subsystem of a bigger system) as a network of smaller systems designed, validated, manufactured with the same or different processes, and tested. Figure 3 shows some of the possible integration methods of dies in a package. From a security perspective, some security requirements may need to be imposed upon the network connecting the dies, since the network exposes information to much easier access by attackers for probing attacks.



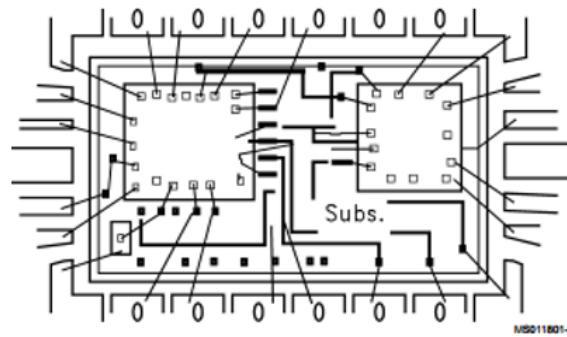
Type 1: Multiple die with die-to-leadframe bonding. No substrate. [3]



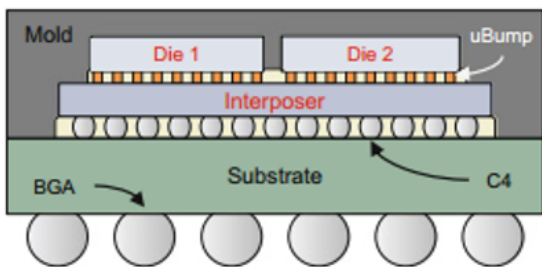
Type 2: Multiple die with die-to-die bonding. No substrate. [3]



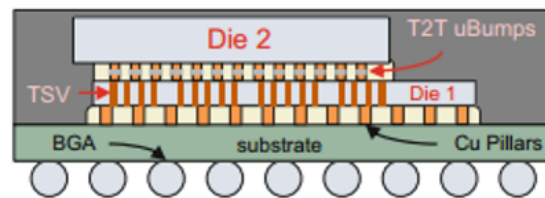
Type 3: Multiple die with jumper chip. No substrate. [3]



Type 4: Multiple die on substrate. [3]



Type 5: Multiple die in 2DS architecture. [4]



Type 6: Multiple die in 3D architecture. [4]

Figure 3. Multiple package types

2. Securing Information Flow among Chips in a Package

Figure 4 shows a bus connecting die A to die B that allows information exchange between them. Here the bus comprises both data and control signals. Although this picture is based on Type 4 of Figure 3, the intention is only to show that two dies are connected by some interconnect that allows information exchange between them; A and B can also refer to any dies on Type 5 (2.5D HI) and Type 6 (3D HI) with vertical interconnects instead of the horizontal interconnects of Type 4. The techniques for securing information flow are applicable to all types, although Type 4 has been used as an example.

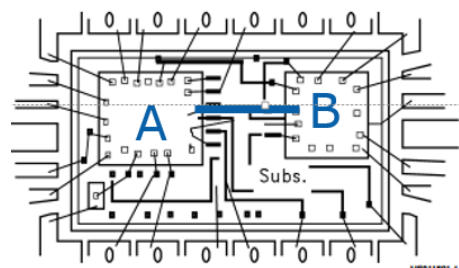


Figure 4. Inter-die information flow between dies A and B [3] with some modifications

To ensure that probing attacks do not compromise the confidentiality of encrypted data, and to mitigate probing attacks, signals with confidentiality requirements should pass between dies encrypted. To ensure that bypassing and/or data injection attacks (Man-In-Middle attacks) cannot modify data in transmission from the sender die to the receiver die without being detected:

- signals with integrity requirements should pass between dies using hash-based message authentication code techniques, and
- signals with both integrity and confidentiality requirements should pass between dies using an authenticated encryption protocol.

3. Techniques to Improve Security against Physical Attacks

As an alternative or complimentary method, the following techniques can be used to detect if a package has been opened or a probing attack is being attempted:

- Anti-tempering sensors should be designed and implemented into dies to notify the security control/monitoring unit of a system that the chip has been depackaged. Sensors: Light sensor, Pressure sensor, Electrostatic or Electromagnetic sensors.
- Active and passive shields can be designed for and implemented into dies to avoid probing attacks.
- A subset of wire interconnects used in dies can be designed in packages similar to split manufacturing techniques. When using such techniques, depackaging can destroy the interconnect subset passing through the package and make it non-functional. (Although reverse-engineering the package allows the network of interconnects to be determined, this method increases the level of security against depackaging attacks.)

4. Techniques to Authenticate Packages

While the methods described in subsections 3.2 and 3.3 focus on security of the information flow on a multi-die package from a supply-chain security perspective, the methods described below are generally employed to authenticate the packages. While our focus is on packages with multiple dies, the methods are applicable to packages with single die as well.

- Printed watermarks on the package, which is the oldest method that has been used for a long time with the least cost and the least security.
- Etched markings on the package.
- Digital holographic watermarks.[5]
- Depositing or etching unique nano-structures on the package.[6]
- Authentication codes based on physical unclonable functions (unique random nano-structures existing on packages).

Note that the latter four techniques have been devised to increase the robustness of packages against supply-chain attacks.

B. Hierarchical/Layered Security

Heterogeneous integration of integrated circuits (IC) and Systems-on-Chip (SoC) from untrusted suppliers exposes the System-in-Package (SiP) to Denial-of-Service (DoS) attacks or unauthorized access to valuable data such as encryption keys or metadata derived from sensor readings. Countermeasures against such attacks can be broadly categorized as always-on or threat-triggered. In the latter case, the system must first detect that it is under attack before activating countermeasures.

A clever attacker may have inserted a hardware Trojan during the manufacturing process for a die, including a mechanism for triggering it later, perhaps in response to the availability of data worth stealing, or in response to data from in-package sensors, such as an altimeter or thermometer. Various methods for detecting Trojans during design verification or post-manufacturing test have been published^[7], but we must assume that the Trojan is hidden well enough to avoid detection until the device is deployed in the field. There is thus a need for research into algorithms for detecting anomalous behavior within and between the sub-system SoC in a SiP, and into how those algorithms can be implemented by security-monitoring software running on a trusted die in the SiP. This trusted die may be responsible for other mission-critical functionality; for example, it can control dynamic voltage and frequency scaling (DVFS) for extending the uptime of energy-constrained systems such as those powered by batteries and/or energy-harvesting devices.

The Security Controller (SC) should be able to control each component die’s access to the power rails as a response to detection of an attack in progress, or as a pro-active measure whenever a die’s authenticity cannot be established. Alternatively, the SC can isolate a suspected die from package-level interconnects, in effect holding it under quarantine until further testing or evaluation of the threat can be completed. In one scenario, the SC might keep a suspected die powered on until security checking is finished, and then decide whether to maintain the power connection or force a power-off event.

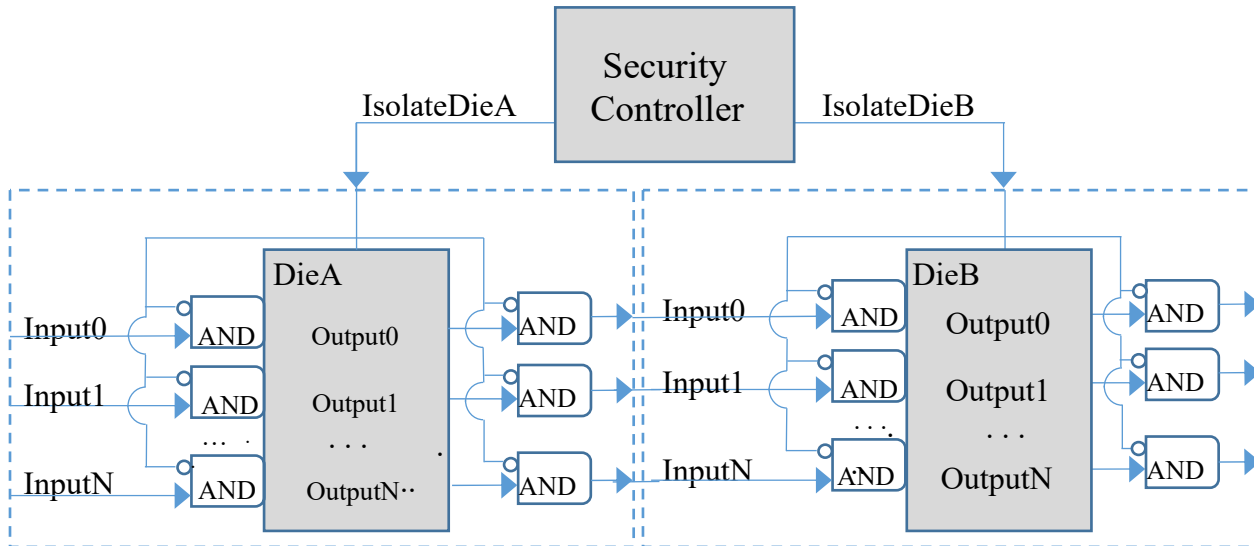


Figure 5: Die-level Isolation using a Security Controller

In the general case, testing of die-to-die and die-to-system connectivity will require the ability to configure each die’s input/output/bi-directional pins as outward-facing (e.g., for IEEE 1149.1’s EXTEST mode), so it should be possible to isolate each component die by leveraging Design for Testability (DFT) hardware already designed into the SiP. P1838, the IEEE standard being developed for stacked integrated circuits^[8], may provide sufficient controllability for isolating a die functionally, but it should not be assumed that P1838-compliant isolation logic can actually be leveraged in anything other than a special test mode; if isolation logic is to be used in response to the identification of a security threat, then the ability of the Security Controller to generate the correct sequence of control signals must be checked during verification. Furthermore, the die isolation circuits must be protected against malicious usage, for example in a Denial-of-Service (DoS) attack which makes the system inoperable by isolating one or more die. Locking Segment Insertion Bits (LSIB) have been proposed^[9] to prevent writing to (or reading from) segments of a control register unless a cryptographic key is provided.

SiP designers may prefer only granting access to the inter-die communication network during brief time periods when data traffic is expected. The mechanism of granting/denying access can be a simple isolation fence, as in Figure 5, with the controlling input signals being generated by the SC. SiP designers can include an override capability in order to enable testing of the package-level interconnect, provided that setting the override bit can only be done if cryptographic authentication is passed (e.g. the correct crypto key is provided), and that the crypto key is only known by the SiP integrator.

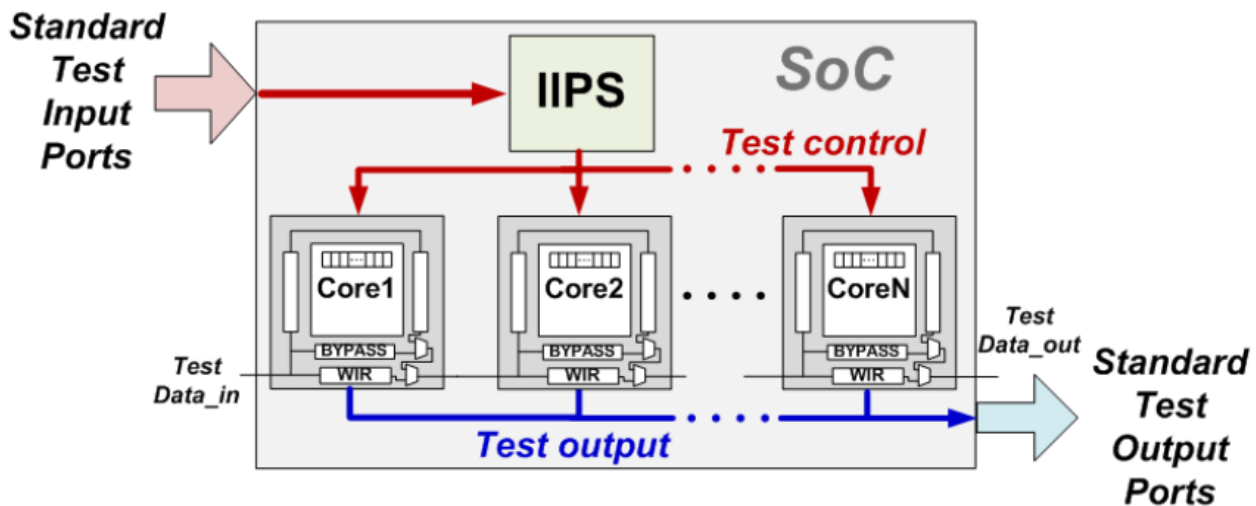


Figure 6: IIPS infrastructure IP for security interfaces with constituent cores of an SoC.[10]

In the following picture, a security controller with similar functionality of the SC has been proposed in the infrastructure IP for SoC Security (IIPS)^[11] as shown in Figure 6. For HI, it is possible to extend the proposed concept, but the differences are (a) there are multiple dies, and (b) one die would be responsible for authenticating the rest of the dies and provide secure communication among them; however, there should be mechanisms to make sure that the security controller cannot be replaced with a counterfeit die, giving false assurance to the users regarding security.

The SC can compute metadata describing the operation of the SiP’s sub-systems (IC/SoC), using metrics such as the number of clock cycles required (or the energy consumed) for completing an algorithm of known length and known input data. The idea behind such a canned test sequence would be that a sub-system might generate noticeably different metadata after its Trojan is triggered, so historical data from previous testing, done at regular intervals, would need to be stored by the SC.

System designers may prefer simply flagging the data generated by a die containing a suspected Trojan as possibly invalid, allowing the suspect die to continue transmitting data values as usual except that the data will be flagged as possibly tainted. The data collected from multiple SiPs can then be evaluated in context, allowing decisions to be made as to whether the sub-system is truly compromised. Historical metadata from each SiP’s SC can be stored and analyzed, and instructions can be sent back to the SC – for example, running the canned test sequences more frequently.

C. Split Manufacturing Concept

The concept of split manufacturing, as shown in Figure 7, was developed to obfuscate the functionality of a silicon chip by separating its wafer manufacturing process between two different foundries, i.e. an insecure front-end foundry and a secure back-end foundry. This approach is becoming increasingly important since many state-of-the-art front-end foundries are becoming distributed throughout the world with reduced levels of security. The approach used in wafer-level split manufacturing is to modify pin assignments, cell placements and rerouting to hide the chip functionality and vulnerability to attack from either one or both manufacturers.

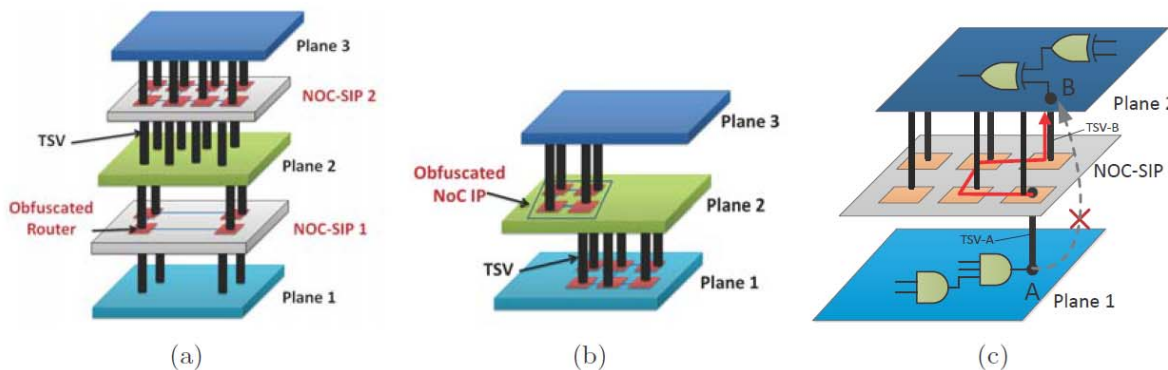


Figure 7: Concept of split manufacturing for security in a 3D stack.[12]

Split manufacturing in the IC world requires high overhead – extremely disruptive and expensive partitioning of the top several metal layers and the underlying process flow between different semiconductor fabs. This partitioning is unnatural and imparts many additional costs, testability concerns and yield ownership issues on the hybrid flows at different fabs. By its very nature, heterogeneous integration at the package level already has to deal with most of these concerns, but to date there has been very little research into the enormous opportunities available for enhanced security using split manufacturing concepts at the HI packaging level. In particular, if appropriately designed for security, HI split manufacturing can offer not just partitioning between two manufacturers, but can partition security between a dozen different chip components with very little increase in cost, area or test complexity. The key is to design security for HI with all of the different chip manufacturers with appropriate encryption keys and interfaces known only to the system integrator. To facilitate testing, limited lifetime keys between required chips could be provided.

To first order, HI split manufacturing design for security can use the concepts of split manufacturing for ICs with none of its additional overhead costs. For example, flexible pin rerouting can be enabled by each chip supplier. These encrypted pin assignment keys would be accessible only to the final system integrator. Having such obfuscation at a dozen different interfaces throughout the system, as opposed to just two interfaces in IC split manufacturing, makes reverse engineering or hacking of these systems much more difficult. It also requires close design-for-security cooperation between many suppliers, integrators and EDA tool vendors – a process that could benefit greatly from road-mapping activities.

Of course, HI split manufacturing design for security is not simply interface pin obfuscation. First, one must understand both current and potential future models for security attacks for such systems. These attacks are dynamic and hard to predict, but a clear understanding of existing attacks and potential vulnerabilities can greatly aid the overall design for system security. There is also a need to develop meaningful metrics to assess the difficulty of an attacker to reverse engineer the properties of these attack surfaces. The split manufacturing concept can also drive key controlled changes in internal functionality of the chips from different suppliers to maximize obfuscation. Incorporation of dynamically configurable components such as FPGAs should also be considered. Engagement of EDA tool vendors in this HI space could provide very obscure and secure changes not only in pin assignments but also in routing, chip functionality and even system architecture. System security improvements as a function of system cost, area and power need to be evaluated.

D. Simulations for EM Side-Channel Attack (SCA) Resilience

Improved simulations for EM SCAs are proposed to reduce the cost and complexity associated with existing EM SCA simulations that require modeling coupling effects, analysis of transient signals at the transistor level, matching circuits, and computing EM fields. The proposed simulation flow for EM is important because it will enable fast and accurate prediction of EM traces, and thus resiliency of these systems to SCA. The cost reduction is achieved via a) use of commercial CAD tools for running transistor-level simulations only during critical times that can leak unintended information; and b) the fact that EM radiation is limited to the currents on top metallization layer power/ground interconnects. The simulations for EM also require that EM traces for different encryption blocks are run in parallel, which greatly reduces the simulation time.

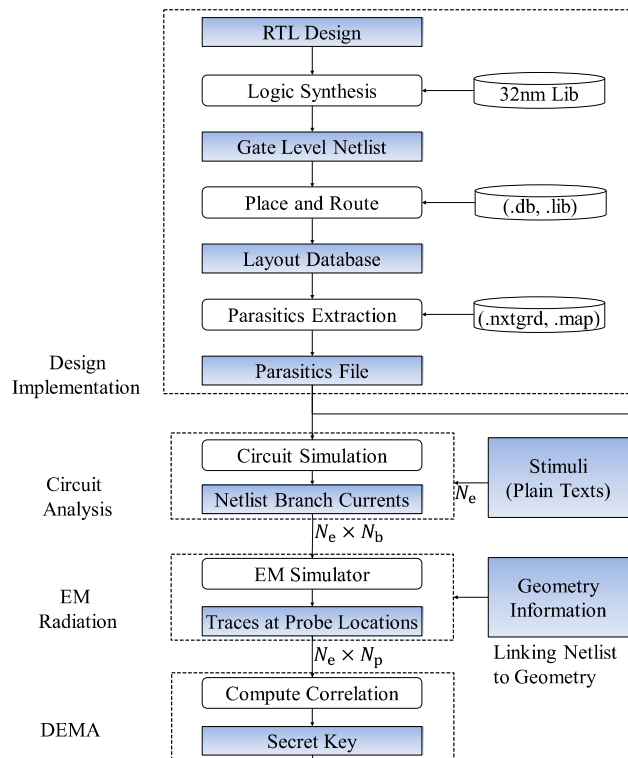


Figure 8: EM side-channel attack vulnerability analysis.[13]

The proposed design flows and the steps for evaluation of SCA vulnerability are shown in Figure 8. It starts with an RTL description of the IC design; however, not all the steps are followed as the differentiated EM attack (DEMA) is focused on the cipher-execution phase that leaks the signal. It has been shown that in case of AES, this occurs in the last round.^[14] The computation of EM signals is also reduced by considering only the currents on the top metallization layer.

The proposed flow analysis allows for parallel execution, which makes it particularly attractive for HI systems. For example, the simulations of EM can run in parallel for every element in the HI system that is implementing an encryption scheme that is observable to an attacker. The approach can identify vulnerabilities with each of the elements in HI and can provide insights on what can be done to improve security of HI. For example, through the use of simulation of EM, it is possible to identify points of vulnerability based on the probe location. By spacing VDD/VSS lines non-uniformly, the number of traces required to break security increases by up to a factor of 5 versus uniform spacing of these lines.^[13]

EM simulations are important since they provide insights into the system vulnerabilities at low cost and high speed. This enables the evaluation of changes to the IC layout design that make EM SCA harder. The current approach is limited to the transmission-line-based EM simulator and full-wave EM simulators which will be required for HI systems. This is important for the complex heterogeneous systems as it will also require predicting vulnerability of communications among different elements in a heterogeneous system.

In general, protections from SCA, such as timing, power, EM, etc., will require countermeasure implementations at several levels^[15]: at the transistor level to reduce leakage, at the program level to randomize operations, at the algorithm level with the objective of reducing leakage, and at the protocol level to limit the computations an attacker can provide with a given key. General SCA protection will require engagement and understanding of security issues by designers and integrators at every level.

Section 4. General Conclusion

Clearly, cybersecurity is an important concern for all electronic systems. The general trends of increasing electronic system complexity and interconnectivity have made cybersecurity one of the top priorities for research, particularly for applications with life-threatening exposure. This chapter has addressed those cybersecurity threats that are most affected by the much broader supply chain, more complex system topology and increased proximity of

chips being driven by heterogeneous integration. As described in detail above, heterogeneous integration has major security impacts due to changes in interconnect layouts, test protocols, supply chain diversification and vertically stacked geometries. It is clear that these increased security threats must be addressed by a more system-level approach to security that requires a systematic design-for-security perspective.

Simply trying to add a patch for security for commodity chips from diverse suppliers with many high-bandwidth interfaces for attack will at best delay the security risks until a new attack vector is discovered. What is really needed is a design-for-security approach at the system level that uses the innovations such as advanced authentication, hierarchical security, split manufacturing concepts, and SCA mitigation strategies to fundamentally change the boundary conditions. To achieve this design-for-security goal for HI at the packaging level, advances in EDA tools at the packaging level are needed with options to trade off system security with other metrics such as performance, power and area. There have been recent advances in package-level design tools, but these need to be augmented with security-centric tests and metrics.

It is important to stress that without appropriate countermeasures, the HI of many chips in close proximity from many different vendors will lead to increased vulnerabilities of these compact IoT systems to cyberattacks. It is only through fundamental understanding, close cooperation between suppliers and proactive system design-for-security innovations that we can provide security enhancements for HI products with minimal negative impact on cost, area, power or performance.

References

- [1] Extracted from “Research Needs for Secure, Trustworthy, and Reliable Semiconductors”, SRC workshop publication, 2013. <https://www.src.org/library/publication/p066751/p066751.pdf#search=research%20needs%20for%20secure%20trustworthy>
- [2] Sohrab Aftabjahani and Steve Brown, “Taxonomy of Physical Attacks,” TrustHub, VulnerabilityDB, 2018. [Online]. Available <http://www.trust-hub.org/vulnerabilityDB.php>.
- [3] Texas Instrument Literature Number: SNOA287. [Online]. Available <http://www.ti.com/lit/an/snoa287/snoa287.pdf>.
- [4] R. Radojic, More-than-Moore 2.5D and 3D Sip Integration, Springer, 2017.
- [5] C.S. Kim, K.H. Jong, and S.J. Im, “Document watermarking based on digital holographic principle”, Institute of Optics, Department of Physics, Kim II Sung University, Pyongyan, DPR of Korea.
- [6] E. Wang and Y. Zhao, “Etching of nanostructures on soda-lime glass”, Optics Letters, Vol 39, 2014, p. 3748-3751.
- [7] R. Elnaggar and M. Tahoori, “Run-Time Hardware Trojan Detection Using Performance Counters”, Proceedings of the International Test Conference, 2017.
- [8] E. J. Marinissen, T. McLaurin and Hailong Jiao, "IEEE Std P1838: DfT standard-under-development for 2.5D-, 3D-, and 5.5D-SICs," 2016 21th IEEE European Test Symposium (ETS), Amsterdam, 2016, pp. 1-10.
- [9] J. Dworak, Z. Conroy, A. Crouch and J. Potter, "Board security enhancement using new locking SIB-based architectures," 2014 International Test Conference, Seattle, WA, 2014, pp. 1-10.
- [10] X. Wang, Y. Zheng, A. Basak and S. Bhunia, "IIPS: Infrastructure IP for Secure SoC Design," in IEEE Transactions on Computers, vol. 64, no. 8, pp. 2226-2238, Aug. 1 2015.
- [11] A. Basak, S. Bhunia, T. Tkacik and S. Ray, "Security Assurance for System-on-Chip Designs With Untrusted IPs," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 7, pp. 1515-1528, July 2017.
- [12] J. Dofe, Q. Yu, H. Zhang, and E. Salman, Proc. Great Lakes Symposium on VLSI (GLSVLSI16), pp. 96-74, May 2016.
- [13] A. Kumar, C. Scarborough, A. Yilmaz and M. Orshansky, "Efficient simulation of EM side-channel attack resilience," 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Irvine, CA, 2017, pp. 123-130.
- [14] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis”, Advances in Cryptology, pp. 789, Springer Berlin/Heidelberg, 1999.
- [15] G. Bertoni, J. Daemen, M. Peeters and G. Van Assche, “Note on side-channel attacks and their countermeasures”, [Online]. Available at <https://keccak.team>

Edited by Paul Wesling