HIR

HETEROGENEOUS INTEGRATION ROADMAP

Security Initiative Update

Security TWG Members:

Sohrab Aftabjahani - Intel Corp., chair

Scott List - Sandia National Labs., last chair

Ariton Xhafa - Texas Instruments

John Oakley - Semiconductor Research Corporation

Joel Irby - Draper

Amitabh Das - Advanced Micro Devices

Navid Asadi - University of Florida

Janusz Rajski - Siemens

TWG Members (from Left to Right)

Sohrab Aftabjahani – Intel Corporation, chair

Scott List – Sandia National Laboratories, founding chair *

Ariton Xhafa – Texas Instruments

John Oakley – Semiconductor Research Corporation

Joel Irby – Draper

Amitabh Das – Advanced Micro Devices

Navid Asadi – University of Florida

Janusz Rajski - Siemens

* Listed as courtesy, but not a member of our TWG anymore.

Security Initiative Working Group

TWG chair: Sohrab Aftabjahani, Intel Corporation

Sohrab is a senior staff security researcher and product security expert with the Data Center Group at Intel Corporation. Since 2010, he has been contributing to its state-of-art R&D projects in various roles including senior security researcher, senior DFT engineer, senior digital design and validation engineer, and graphics integration validation engineer. He is a senior IEEE member and a senior ACM member. He authored 39 papers, book chapters, technical reports, and a patent. His PhD is in Electrical and Computer Engineering from the Georgia Institute of Technology.

TWG previous chair: Scott List, Sandia National Laboratories

Scott was the Director of Trustworthy and Secure Semiconductors and Systems (T3S) and Innovative and Intelligent Internet of Things (I3T). Prior to joining SRC, Dr. List was with Intel's Components Research department for 18 years with management responsibilities including university research, nano-metrology development, 3D IC research, advanced interconnect solutions, decoupling capacitor integration, Intel's 45 nm silicon technology roadmap, high frequency measurements/simulation and Cu integration.

Updates

Chapter Outline (2023)

I. General Cybersecurity Hardware Challenges and Needs (Revised)

II. Specific HI Cybersecurity Needs (Expanded)

III. Specific HI Security Opportunities

IV. General Conclusions

Cybersecurity Attacks / Impacts / Mitigation

Hardware Attack Vector	Impact	Mitigation Strategy
Interface Leakage	Unauthorized access directly at interfaces or through test/debug mechanisms/interfaces	Design for security, interface obfuscation
Supply Chain Attacks	Hidden/delayed, unwanted functionality or security (confidentiality, integrity , or availability) compromise, Trojans, etc.	Design validation, parasitic detection, active triggering at test or validation, IP/Design/Materials Provenance
Side Channel Attacks (SCA)	Access to secure information such as encryption keys	Making designs SCA-resistant by analyzing side-channel leakage (timing-based, power-based, electromagnetic, acoustic, optical, thermal) of design through simulations to determine the leaky side channels and block them to avoid leakage of sensitive information
Chip Counterfeiting	Unauthorized use of aged or production of duplicate or compromised chips	Secure chip odometers and unique authentication based on Physical Unclonable Functions (PUF)
Physical Tampering	Invasive access to secure information including reverse engineering	Sensors which detect intrusion and activate safe mode defaults
Fault Injection Attacks	Compromising 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 1) determine the functional elements and their interactions; 2) get access to embedded secrets; 3) find vulnerabilities and weaknesses; 4) launch other attacks such as fault attacks, physical attacks, and side channel attacks; or 5) discover effective targets for physical tampering or chip counterfeiting	Tamper-proof fixtures and layout obfuscation such as blind/buried vias

First Order Security Impacts to Other TWGs

Associated HIR TWG	First Order Security Impacts
Single Chip and Multi Chip Packaging	Additional interface, information flow and authentication concerns
Integrated Photonics	SCA of optical fibers requires closer proximity than that for EM SCA
Integrated Power Devices	DP SCA at a more local scale is 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 potentially making SCA easier due to EM radiation
Materials and Emerging Research Materials	Integration of magnetic materials can better shield EM signal [we can add a reference / active package]
Emerging Research Devices	Qubits and entangled communications/emerging NVM can set new security paradigms
Interconnect	Major effects from chip interconnectivity possibly increasing attack surface and vulnerabilities (see below)
Test	Flexible test methodologies without secure design exacerbate vulnerabilities (see below)
Supply Chain	Multiple suppliers for multiple chips necessitates new interface controls (see below)
Security Initiative	System design for security is becoming an imperative
SiP	Increased proximity and connectivity of chips from diverse suppliers may present increased risks
3D + 2.5D	Testability requires some access to each die. Increased proximity can ease SCA (see below)
WLP	Easier access to connectivity of chips may present increased risks
Mobile	Increased proximity and connectivity of chips from diverse suppliers may present increased risks
IoT	Increased proximity and connectivity of chips from diverse suppliers may present increased risks
Medical and Health	Life threatening risks need increased security partitioning and fail-safe operation (see below)
Automotive	Life threatening risks need increased security partitioning and fail-safe operation (see below)
High Performance Computing and Data	High inter-chip bandwidth poses unique security screening challenges
Aerospace and Defense	Life threatening risks need increased security partitioning and fail-safe operation (see below)
Co-Design and Simulation	System design for security is becoming an imperative (see below)

TWG Progress – Chapter Update

- Improved the technical writing as well as some terminologies
- Updates on Post-Quantum Cryptography based on the most recent NIST announcements
- Updates on Lightweight Cryptography
- Updates on Security of Interconnects and Supply Chain Security of Chiplets (Universal Chiplet Interconnect Express (UCIe), which is a plug-and-play interconnect at the package level supporting PCIe, CXL, and raw mode)
- Updates on Secure Test/Debug
- Updated HI Security Pre-competitive Research Areas
- Updated HI Security/Metrology Roadmap

Updates

Cybersecurity HW Challenges

MTG

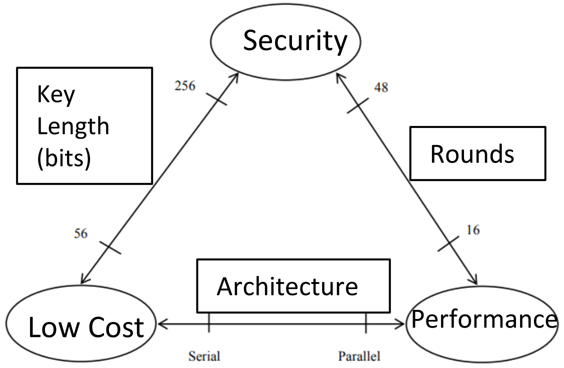
- Post-Quantum Cryptography (PQC)
  - Sufficient qubit Quantum computers expected to come in a decade -> breaking traditional public key cryptography -> needing quantum-attack secure crypto algorithms.
  - Updates: NIST selected candidates:
    - Key Encapsulation Mechanism (KEM)/Public-key Encryption, and Key-establishment Algorithm: Crystal Kyber (Lattice-based)
    - Digital Signature algorithms (DSA): Crystals Dilithium (Lattice-based), Falcon (Lattice-based), Sphincs+ (Hash-based)
  - NIST draft PQC standards with specific algorithm parameters were planned for 2023 inviting public comments, and the standards are going to be finalized in 2024

Updates

HETEROGENEOUS INTEGRATION ROADMAP

Cybersecurity HW Challenges

- Lightweight Cryptography
  - Most lightweight crypto algorithms being standardized by NIST are authenticated encryption ciphers. Suitable for short messages. Can be used for link layer (PCIe/CXL/IDE)) encryption/authentication. Encryption key rolling is a side-channel attack mitigation for low-cost side-channel countermeasures of the link.
  - Updates: ASCON was announced by NIST as selected candidate from 10 finalist algorithms and consists of:
    - Authenticated encryption schemes with associated data (AEAD)
    - Hash functions (HAS) and extendible output functions (XOF)
    - Pseudo-random functions (PRF) and message authentication codes (MAC)
  - Advantages of ASCON:
    - Inherent side-channel protection,
    - Very efficient bit-sliced implementation of the S-boxes (prevents timing attacks, since no lookup tables are required)
    - Low algebraic degree of the S-box (5-bit S-box) facilitates both first- and higher order protection using masking or sharing-based side-channel countermeasures

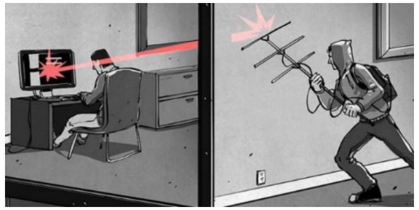


Secure Data Aggregation ...

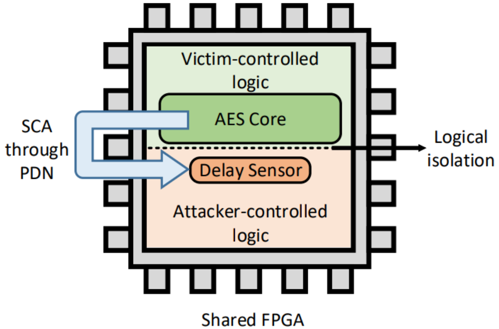
Cybersecurity HW Challenges

- Side-Channel Analysis (SCA) and Fault injection
  - Through Power supply, one chiplet can leak information to the other one. Increased coupling capacitance and inductance in HIR could create unwanted side channels. Embedding MEMS into the package as analog sensors can be used as transducers can leak information.
  - Updates: Combined side-channel attacks are getting more popular. Performance related counters are used for SCA. Adding delay to interconnect buses is used to mitigate electromagnetic side-channel attacks.

- Multi-tenancy security (FPGAs/GPUs)
  - One can leak information to the neighboring tenant through power and electromagnetic side-channels. Domain isolation using static/dynamic partial configuration can provide limited mitigations.
  - Updates: More references were added.
  - Monitoring circuits can be employed to detect unauthorized accesses.



TEMPEST: A TIN FOIL HAT ...



Shared FPGA

Security of Cloud FPGA's ...

Updates

Cybersecurity HW Challenges

Package Interconnect

- Security of Interconnects and Supply chain security of chiplets
  - Protocols such as (a) Integrity and Data Encryption (IDE) for creating secure channels with integrity requirement and (b) Security Protocol and Data Model (SPDM) to attest different chiplets on a package (Key management is important for such protocols.) and (c) Compute Express Link (CXL) security for Universal Chiplet Interconnect Express (UCIe).
  - Updates: UCIe can take advantage of the CXL security. UCIe is an interconnect specification for a die-to-die interconnect and serial bus between chiplets.
    - Supports multiple protocols (PCIe, CXL, and a raw mode that can be used to map any protocol of choice as long as both ends support it) on top of a common physical and Link layer.
    - Security aspects for UCIe need to be considered and integrated into the protocol, especially in the context of complex chiplet-based heterogeneous systems. UCIe can reuse CXL security features.
  - More on UCIe: It is an open, multi-protocol capable, on-package interconnect standard for connecting multiple dies on the same package. It enables a vibrant ecosystem supports disaggregated die architectures offering a plug-and-play interconnect at the package level (chiplets from different sources, including different fabs, using a wide range of packaging technologies.) It addresses the compute, memory, storage, and connectivity needs across the entire compute continuum, spanning cloud, edge, enterprise, 5G, automotive, high-performance computing, and hand-held segments.

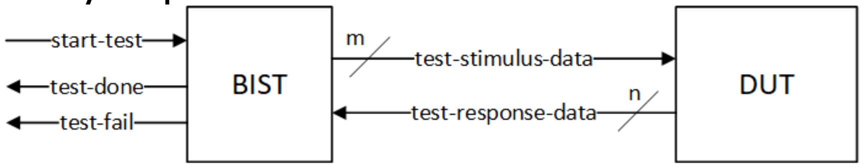
Updates

HETEROGENEOUS INTEGRATION ROADMAP

Cybersecurity HW Challenges

Design for Test
vs
Design for Security

- Secure Test/Debug
  - Test/Debug requires maximum controllability and observability of system (interconnects and components) whereas security requires closing controllability and observability gaps for assets.
  - Updates: Reconciling Test/Debug & Security
  - Enforce access control to access to scan chains (minimize attack surface by restricting it to trusted users), which are used for high quality test. 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.



  - Use a variety of Built-in Self Test (BIST) to achieve high quality test coverage while minimizing attack surface. They include: Logic BIST for random digital logic targets, Memory BIST for arrays such as SRAMs, and AMS/ Analog BIST for and analog/mixed signal (AMS) blocks or even entire chiplets (AMS/Analog BIST).
  - It is also possible to test an IP or chiplet. Pass/Fail results for the IP/chiplet are obtained by one or more of the above BIST mechanisms without exposing information about the internal circuitry to external observers.

HI Security Pre-competitive Research Areas

1	**Trusted architectures and hardware designs**
1.2	Innovative defense mechanisms against “side channel attacks” and elimination of attack vectors
1.3	Cryptographic architectures and designs for either classic security mechanisms or mechanisms to compute on encrypted data, optimized for highly constrained devices, or high-energy efficiency, or high-performance [Light-weight Cryptography]
1.4	Security architectures for heterogeneous systems including protection of AI/ML enabled sub-systems and neuromorphic architectures
1.6	Hardware design strategies and cryptography methods for Post-Quantum, and privacy-preserving devices
2	Security techniques for advanced technologies and packaging
2.3	Security of disaggregated/heterogeneous systems, e.g., advance packaging technologies like heterogeneous integration
5	Authentication, attestation, and provisioning
5.1	Novel approaches to design elements that enable authentication/attestation during design, operation, firmware, operating systems, and throughout the product life cycle (5-20 years), particularly in the cloud environment

SRC Hardware Security (HWS) Call for Research (Research Program Needs 2022) [A Subset chosen interacting with HI Security])

Updates

HI Security/Metrology Roadmap

	Area		Sub-area	2025	2030	2035
1	Cryptography + Cipher/Side Channel Strength	a.	Post Quantum(PQ) Cryptography	In 2022, NIST has finalized the list of candidates: CRYSTALS-KYBER, CRYSTALS-DILITHIUM, FALCON, SPHINCS+ (Alternate candidates will be finalized later)	New attacks may be proposed, and new countermeasures may be required if vulnerabilities are identified in the newly-formed standards. Accordingly, some of the algorithms may be replaced.	TBD
		b.	Lightweight(LW) Cryptography	NIST may give the list of candidates to be finalized.	New attacks may be proposed, and new countermeasures may be required if vulnerabilities are identified in the newly-formed standards. Accordingly, some of the algorithms may be replaced.	TBD
		c.	Side Channel Attacks (SCAs)	Some PQ and LW crypto candidates have inherent side-channel countermeasures or may provide enhancements with existing side-channel mitigations. Even now, new SCAs & new mitigations have proposed targeting GPUs and AI accelerators.	Will have better visibility on attacks and propose practical countermeasures for attacks on CPUs, GPUs FPGAs and accelerators (including AI).	TBD
2	CAD for Security + Quality of Assurance	a.	Tools for automation of security assurance of IPs in context of ASIC/FPGA	EDA tools with basic features (+ pre-Si side channel analysis) Standards for security specification (like IEEE P3164) will be out and EDA tools to support them will be developed.	EDA tools with advanced features and enhanced scalability. Standards for security specification will get mature and EDA tools to support them will be developed.	TBD
		b.	Integrated DFX and Security analysis Tools:	EDA tools with basic features. Standards for security specification will be out and EDA tools to support them will be developed.	EDA tools with advanced features and enhanced scalability. Standards for security specification will get mature and EDA tools to support them will be developed.	TBD
3	Packaging + Quality of Security	a.	Packages supporting EM shields	Simple forms of such packages are being developed.	Advanced forms of such packages will be developed to mitigate SCA and physical attacks.	TBD
		b.	Active Interposers	Simple forms of such interposers are already out.	Advanced forms of such interposers will be developed to mitigate SCA and physical attacks.	TBD

New Challenges and Innovations

- Threat Modelling of HI Systems
- New attacks on Post-Quantum/Lightweight Cryptography final/candidate standards and their mitigations
- New Physical attacks, Fault-injection attacks, and Side-Channel attacks in the scope of the HIR and their mitigations
- Multi-tenancy trend of using FPGAs, GPUs (in general XPUs) to build accelerators in Clouds and High-Performance Computing and its security aspects
- Security of Chiplet interconnects (including new and future standards)
- Design for Test and Test of Heterogenous Integrated Systems and its interactions with security

Cross TWGs Collaborations

- Coauthoring (Security and Privacy Chapter) of NIST Microelectronic and Advanced Packaging Technologies (MAPT) Roadmap through collaboration of several member of our TWG (Sohrab, Amitabh, and Navid) and several our [SRC Hardware Security program] academic collaborates / university professors (Farimah Farahmandi, Mark Tehrani-Poor, Navid Zanjani, Prabhat Mishra) and other participants (from industry, government, and academia).

- Not direct collaboration with other TWGs this year but indirect collaboration through academic collaboration with an army of security researchers.

- Open for collaboration with all other TWGs in 2024.

NIST Microelectronic and Advanced Packaging Technologies (MAPT) Roadmap

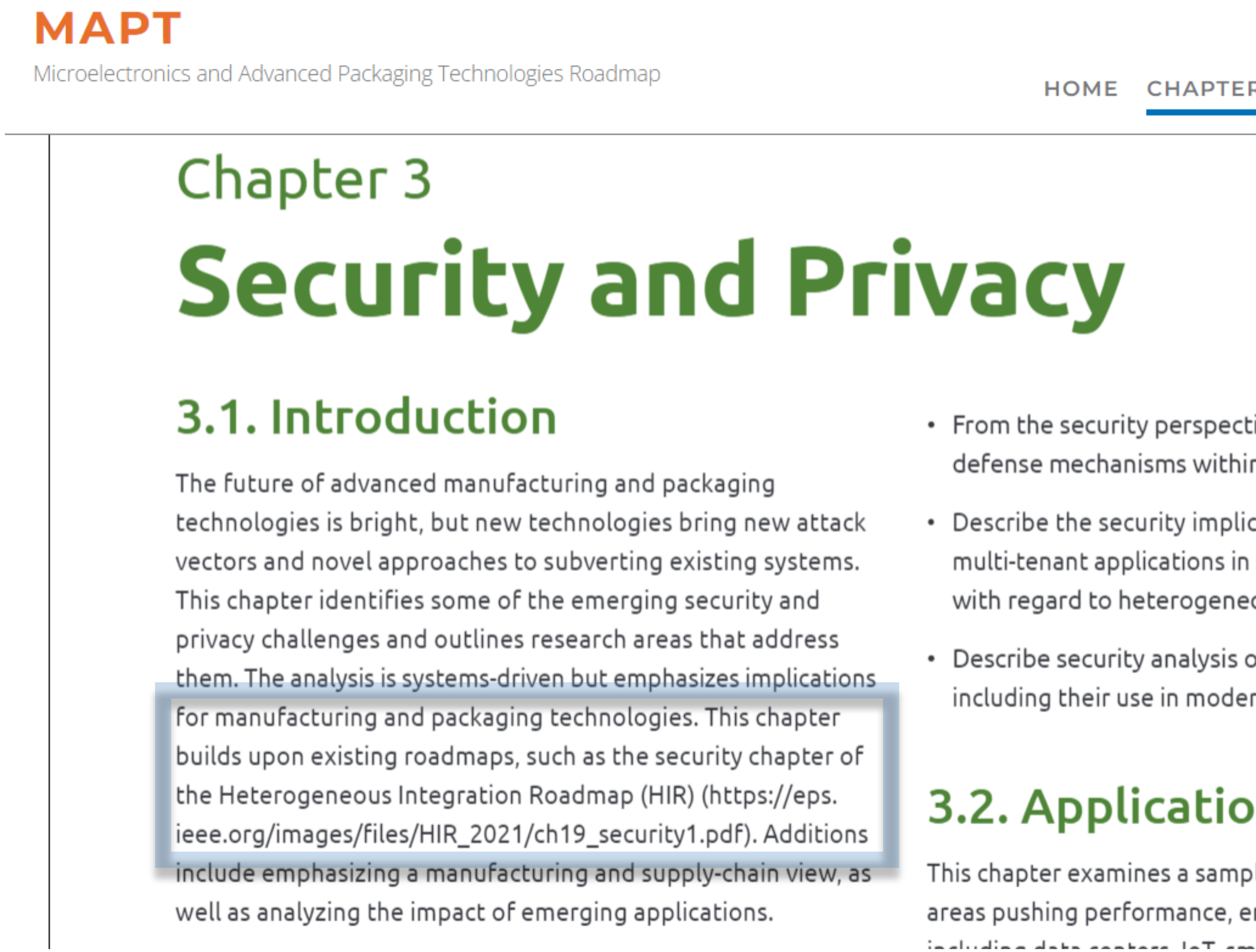
- MAPT Roadmap Technical Working Groups
  - TWG A: Workforce Development
  - TWG B: Application Drivers & System Requirements
  - TWG C: Advanced Packaging & Heterogeneous Integration
  - TWG D: Digital Processing
  - TWG E: AMS Processing
  - TWG F: Photonics & MEMS
- Crosscuts
  - Crosscut I: Manufacturing and Process Metrology
  - Crosscut II: Sustainability & Energy Efficiency
  - Crosscut III: Design, Modeling, Test, and Standards
  - Crosscut IV: Supply Chain: Materials, Chemicals, Substrates
  - Crosscut V: Security and Privacy

" Advanced Packaging, along with 3D monolithic and heterogeneous integration, will be the key enabler of the next microelectronic revolution. In fact, advanced packaging+3D is becoming the equivalent of transistor of the 2D Moore's Law era. This initiative closely aligns with SRC's Decadal Plan, which stresses the urgency of increased research funding in this area. "

Source: NIST Microelectronic and Advanced Packaging Technologies (MAPT) Roadmap

MAPT Security and Privacy Chapter

- System driven analysis (Application Drivers) with emphasis on implications for manufacturing and packaging technologies
- Built upon our HIR Cybersecurity chapter
- Emphasizing manufacturing and supply-chain view and analyzing the impact of emerging solutions



MAPT

Microelectronics and Advanced Packaging Technologies Roadmap

Chapter 3

Security and Privacy

3.1. Introduction

The future of advanced manufacturing and packaging technologies is bright, but new technologies bring new attack vectors and novel approaches to subverting existing systems. This chapter identifies some of the emerging security and privacy challenges and outlines research areas that address them. The analysis is systems-driven but emphasizes implications for manufacturing and packaging technologies. This chapter builds upon existing roadmaps, such as the security chapter of the Heterogeneous Integration Roadmap (HIR) (https://eps.ieee.org/images/files/HIR_2021/ch19_security1.pdf). Additions include emphasizing a manufacturing and supply-chain view, as well as analyzing the impact of emerging applications.

- From the security perspecti defense mechanisms withi
- Describe the security implic multi-tenant applications in with regard to heterogene
- Describe security analysis o including their use in mode

3.2. Applicatio

This chapter examines a samp areas pushing performance, e

Events or activities in the industry

- Ongoing Rev 2 Parallel Road mapping Effort: NIST Microelectronic and Advanced Packaging Technologies (MAPT) Roadmap – Sohrab, Amitabh, and Navid contributed to its Crosscut VI (Security and Privacy).
- Workshop: Secure Heterogeneous Integration Workshop, May 1st, 2023 at the IEEE International Symposium on Hardware Oriented Security and Trust (HOST) by the University of Florida Professors (Mark Tehranipoor and Farimah Farahmandi).
- RESHAPE: Reshore Ecosystem for secure Heterogenous Advanced Packaged Electronics at the IEEE International Conference on PHYSICAL ASSURANCE and INSPECTION of ELECTRONICS (PAINE) 2023 by Alexander Quadrini – Army.
- Keynote Talk IV: Challenges and Opportunities for 3D Heterogeneously Integrated Microsystems at the IEEE International Conference on PHYSICAL ASSURANCE and INSPECTION of ELECTRONICS (PAINE) 2023 by Dr. Anna Tauke-Pedretti – DARPA.
- Enabling Security of Heterogeneous Integration: From Supply Chain to In-Field Operations, IEEE Design & Test (Volume: 40, Issue: 5, October 2023) by Professors of the University of Florida(Mark Tehranipoor, Farimah Farahmandi, etc.).
- Heterogeneous Integration Supply Chain Integrity Through Blockchain and CHSM, ACM Transactions on Design Automation of Electronic Systems by Professors of the University of Florida(Mark Tehranipoor, Farimah Farahmandi, etc.) .
- ToSHI - Towards Secure Heterogeneous Integration: Security Risks, Threat Assessment, and Assurance by Professors of the University of Florida(Mark Tehranipoor, Farimah Farahmandi, Navid Asadi) and their team.

Modernizing our Collaboration Space

- We created a Workgroup Space for HIR Cybersecurity WG in 2022.
- Professor Navid Asadi, University of Florida, allocated a Microsoft-Teams space to our TWG. It is owned by an academic entity vs participants from Industry who might have limitations on allowing access to their competitors and protect their IPs. It allows access to the space while keeping the Microsoft Teams space of the companies/organizations separate.
- This model allows creating access-controlled channel for discussions on various topics.
- The workspace is managed by Navid. The content is maintained by our TWG. University of Florida IT maintains its supporting IT infrastructure.
- We propose other TWGs to create similar working spaces or create one for all TWGs of the HIR through the University of Florida (if they agree) or other academic research centers or organizations.

General HI Security Conclusions

- HI-induced changes in interconnect geometrical layouts, increases in the number of connections and bandwidth between chips, complexity in system test protocols, and supply chain diversification and encryption key access, present major challenges to cybersecurity.

- HI system security advances using evolutionary changes will only provide marginal benefits.

- A system-level design for security approach will be needed to mitigate these threats and will require close interactions between chip designers, chip manufacturers, system integrators and system level EDA tool vendors.

- Full cooperation in the system-level design for security can use the multi-chip and diverse supplier nature of HI to actually enhance the system security.

HI Security Call to Action

To achieve these close interactions between HI chip designers, chip manufacturers, system integrators and system level EDA tool vendors:

1) We must quantify potential benefits of HI system level security threat mitigation strategies versus associated performance, power and area costs.

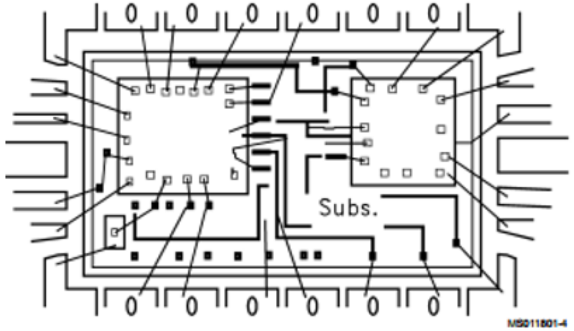
2) Initially, HI chip vendors with the advanced security features at their interfaces will provide a differentiating competitive advantage.

3) Eventually, all HI chips will require these advanced security features, i.e. design for security will become a requirement.

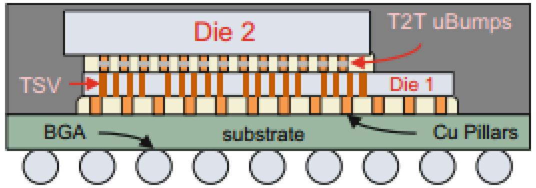
Backup Slides

- Securing Information Flow
- Die-level Isolation by Security Controller
- Split Manufacturing Concept
- EM Side Channel Attack Resistance
- Security for Test/Debug Modes
- Physical Assurance for HI Packaging - Supply Chain Attack Classes
- Physical Assurance for HI Packaging - Taxonomy of physical inspection for material and structure characterization

Securing Information Flow



Texas Instruments Literature Number: SNOA287. [Online]. Available http://www.ti.com/lit/an/snoa287/snoa287.pdf.



R. Radojcic, More-than-Moore 2.5D and 3D Sip Integration, Springer, 2017.

Differentiating Features

- Multiple (2) die,
- T2T uBumps,
- TSV's,

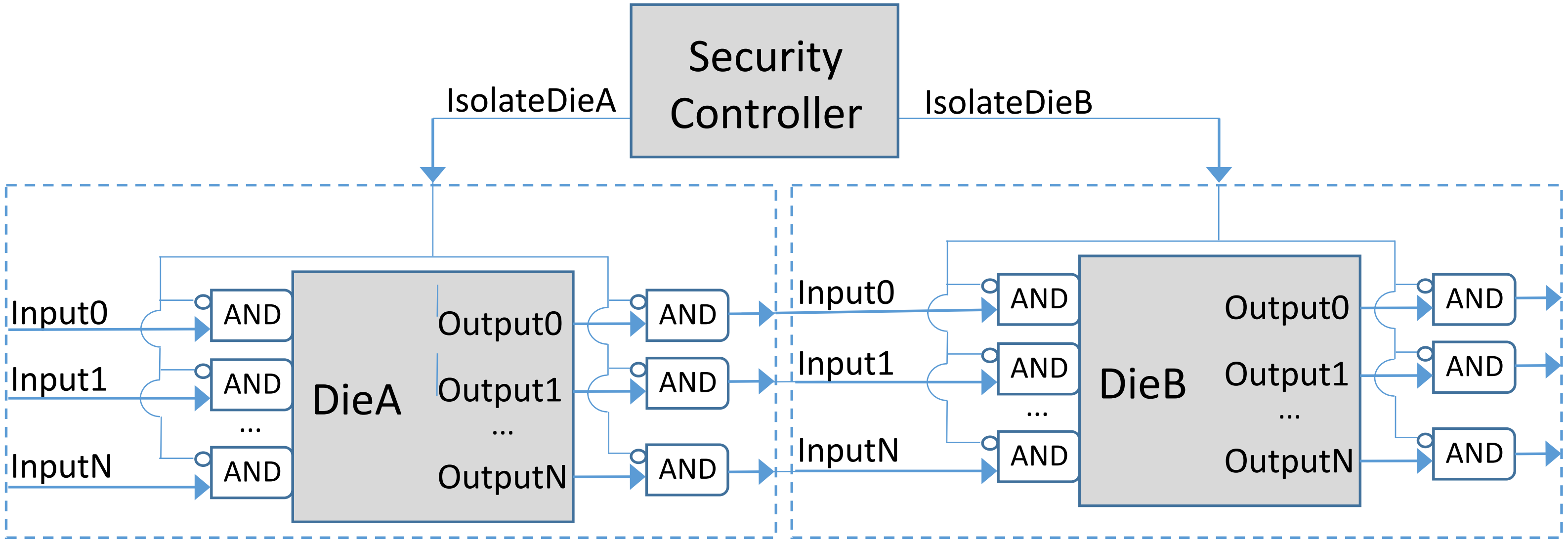
Control of Information Flow:

- Signals with integrity requirements should pass between dies using hash-based message authentication code techniques.
- Signals with both integrity and/or confidentiality requirements should pass between dies using authenticated encryption protocols.

Techniques to Improve Security against Physical Attacks

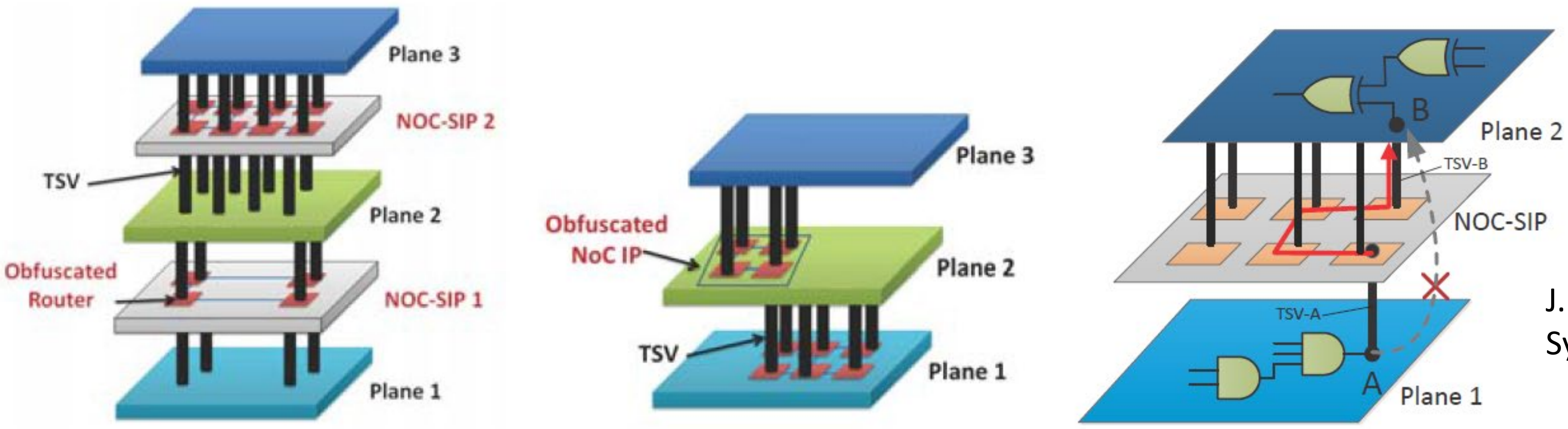
- Anti-tampering sensors should be designed and implemented into dies to notify the security control/ monitoring unit when a system has been depackaged.
- Active and passive shields can be designed for and implemented into dies to avoid probing attacks.
- A subset of wire interconnects used in dies can be designed in packages similar to split manufacturing techniques.

Die-level Isolation by Security Controller



- Security controller die needs to authenticate all other dies and provide secure communication among them.
- Security controller controls each component die’s access to power to provide for isolation control and monitor power profile versus expectation.
- Monitors metadata (energy, clock cycles, or EM) for algorithm for unusual activity.
- Pins can be dynamically reconfigured as input/output or bi-directional to enhance isolation.

Split Manufacturing Concept

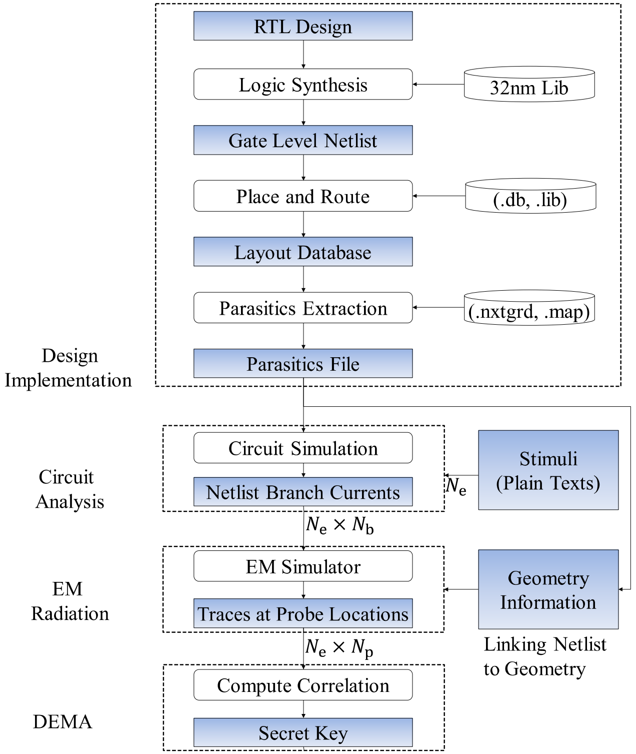


(a) (b) (c)

J. Dofe, et. al., Proc. Great Lakes Symposium on VLSS, pp. 96-74, May 2016.

- Use interface obfuscation in the package or 3D stack similar to split manufacturing on wafer.
- Does not suffer from additional testability, yield and cost issues associated with the partitions on wafer.
- Use each interface to obfuscate pin layouts and system functionality.
- Pin assignments and routing can be controlled by encrypted keys known only to the system integrator.
- Need to design for obfuscation at the package or 3D stack level to maximize effectiveness.

EM Side Channel Attack Resistance



- Efficient simulations of EM signatures for side channel attack vulnerability.
- Feedback to design layout to obfuscate EM patterns, i.e. non-uniform power/ground spacings.
- Efficient approaches to include full-wave simulations beyond traditional TL simulations for the most sensitive traces.
- Program level to randomize operations, algorithm level to reduce EM leakage, and protocol level to limit attacker access with a given key.

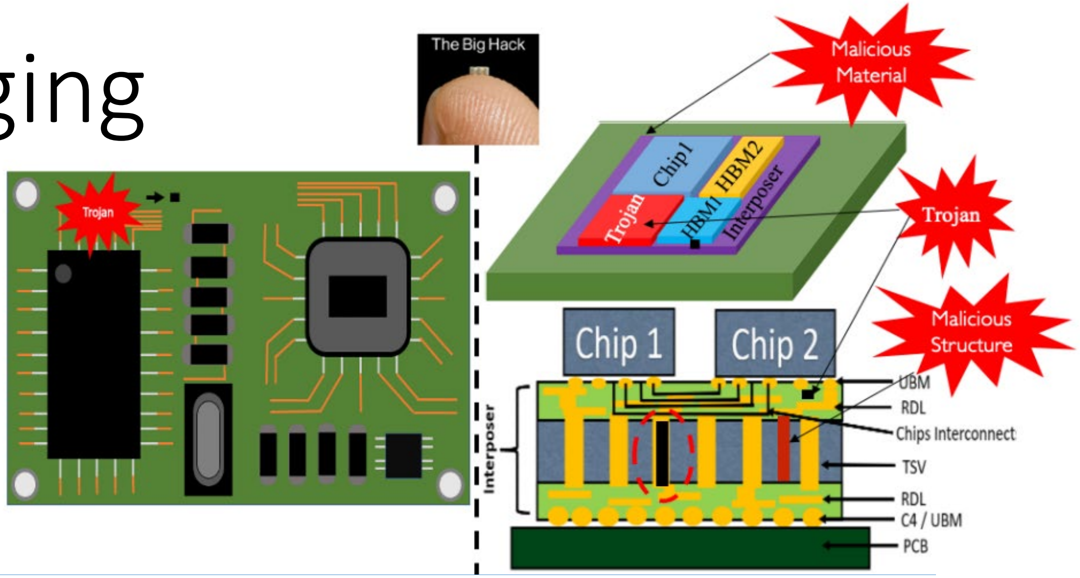
A. Kumar, C. Scarborough, A. Yilmaz and M. Orshansky, 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Irvine, CA, 2017, pp. 123-130.

Security for Test/Debug Modes

- Tests
  - Functional
  - Structural (Random logic (gates, transistors, wires, etc), Embedded memories (SRAM arrays)
- Inputs come from Automatic Test Equipment (ATE). Results sent back to ATE.
- Testing can be use for reverse engineering of the logic (IP theft).
- Logic locking is used to thwart this attack trading area and static power off for security.
- Multiple Input Signature Registers (to compact test output) can be used to capture a known predictable signature for a fault free circuit. For die-stacks, it prevents other dies from having access to the test results of a die; however, it makes defect diagnosis difficult.
- P2929 Scan Dump – Uses MBIST array dump. Access control to restrict access to the dump w/ possible secrets – fuses to disable the access. Fuse override for RMA (part returns)
- IEEE 1149 (JTAG), IEEE 1687 ((jJTAG), IEEE 1500, etc. – iJTAG has the concept of Segment Inclusion Bit (SIB) to include a segment in the chain. Attackers can determine the positions of the bits to enable them by experimentation to unlock a segment.
- RTL level security validation is mostly blind to the DFT inserted into the circuit in physical design space. CAD tools to analyze the final circuit for security can help mitigate possible security risks.

Physical Assurance for HI Packaging

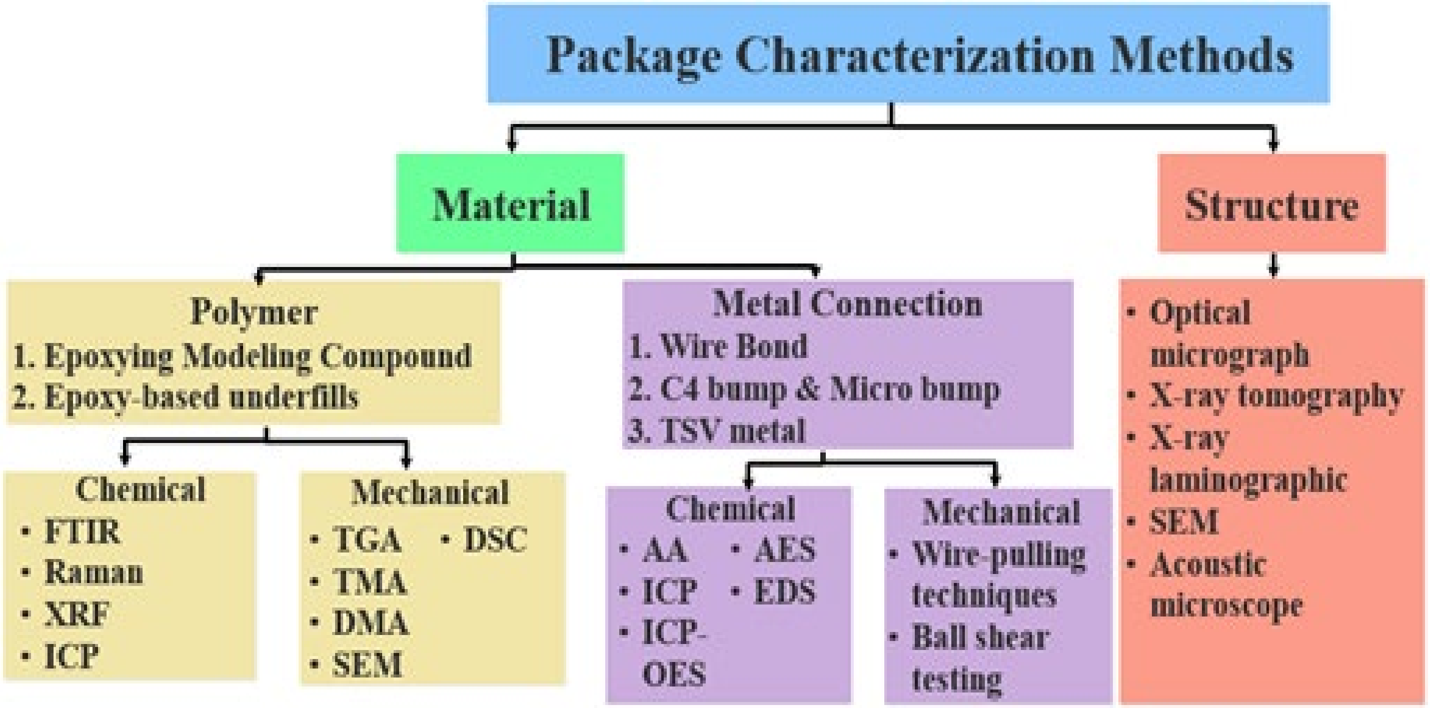
- Supply Chain Attack Classes



HW Attack Vector	Impact	Assurance Strategy
Interconnection Modification	Data leakage, Power malicious components / trojans, Cross talk	"Fully automatic and rapid" interconnect validation using novel "multi-mode" acquisition and analysis inspection techniques: X-Ray, SEM, THz-TDS, etc., combined with novel computer-vision/machine-learning methods
Material Manipulation	Long-term/short-term failures, Denial of service	Develop novel non-destructive characterization methods, Design inherently unique material validation for HI
Hardware Trojan	Data leakage, Key extraction	Develop AI embedded inspection tools for volumetric physical analysis of HI chips

Physical Assurance for HI Packaging

- Taxonomy of physical inspection for material and structure characterization



Package Characterization Methods

Material

Polymer
1. Epoxying Modeling Compound
2. Epoxy-based underfills

Chemical
- FTIR
- Raman
- XRF
- ICP

Mechanical
- TGA
- DSC
- TMA
- DMA
- SEM

Metal Connection
1. Wire Bond
2. C4 bump & Micro bump
3. TSV metal

Chemical
- AA
- AES
- ICP
- EDS
- ICP-OES

Mechanical
- Wire-pulling techniques
- Ball shear testing

Structure
- Optical micrograph
- X-ray tomography
- X-ray laminographic
- SEM
- Acoustic microscope