جامعة نيويورك أبوظبي
NYU | ABU DHABI

CENTER FOR CYBER SECURITY

DFX LAB
DESIGN FOR EXCELLENCE

Hardware Trojan Threats to Cache Coherence in Modern 2.5D Chiplet Systems

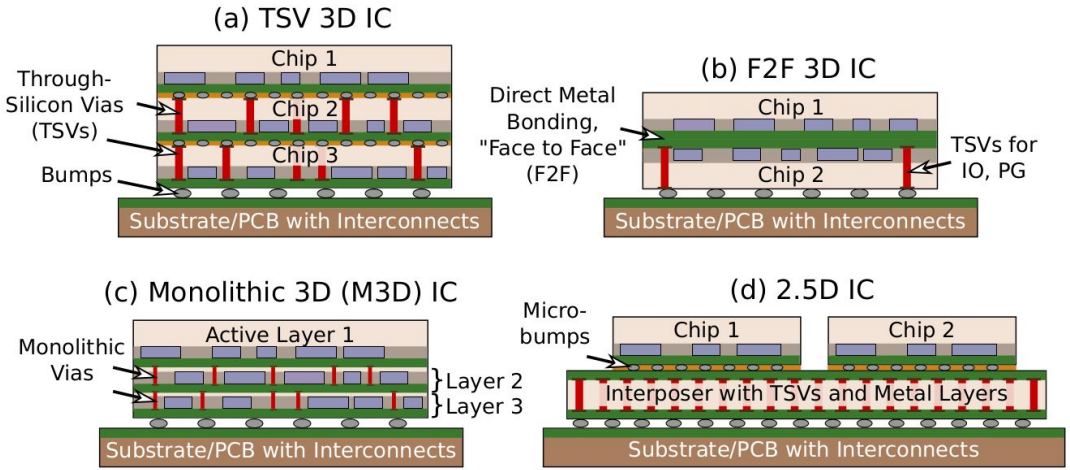
Johann Knechtel
johann@nyu.edu
wp.nyu.edu/johann

HARRIS 2025

Introduction

2.5D, 3D Integration

- Stacking and interconnecting of chips or active layers
- Shorter, vertical interconnects: power consumption, delay, bandwidth – “More Moore”
- Separate dies: heterogeneous and larger systems, yield, ***security*** – “More than Moore”
- But, more complex design, design automation, and manufacturing processes



Knechtel et al., 3D Integration: Another Dimension Towards Hardware Security, IOLTS 2019

2.5D, 3D Integration

Intel Goes Vertical, Will Stack Logic Chips Into 3D Packages

Michael Feldman | December 13, 2018 05:37 CET

GlobalFoundries, Arm Close in on 3D Chip Integration

3D interconnects could shorten delays within processor cores

DESIGNLINES | SOC DESIGNLINE

Intel Steps Toward Heterogeneous Integration

By Dylan McGrath 12.12.2018 1

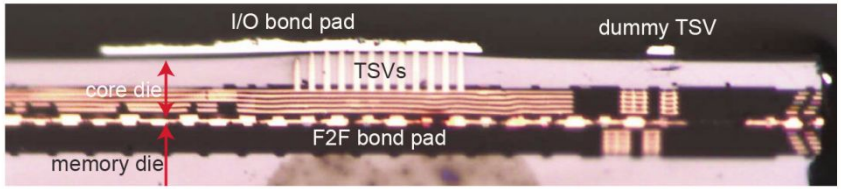
Share Post Share on Facebook Share on Twitter

New 3D packaging technology for face-to-face stacking of logic scheduled to be available in the second half of next year.

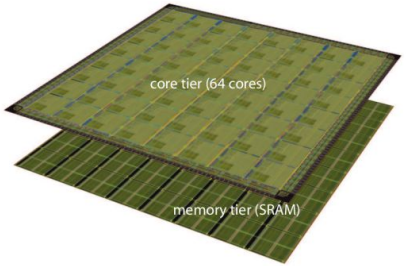
Cadence 3D-IC Advanced Packaging Integration Flow Certified by Samsung Foundry for its 7LPP Process Technology

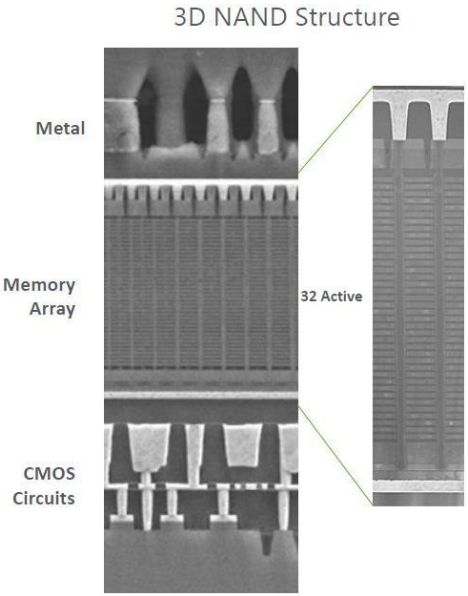
Published: Oct 17, 2019 10:45 a.m. ET

2.5D, 3D Integration

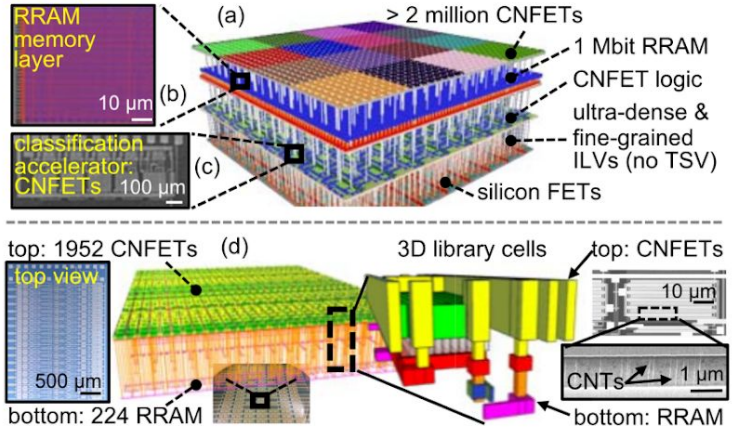


Kim et al., ISSCC, 2012

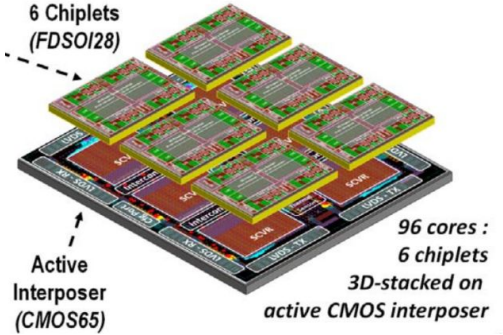




https://www.anandtech.com, 2016



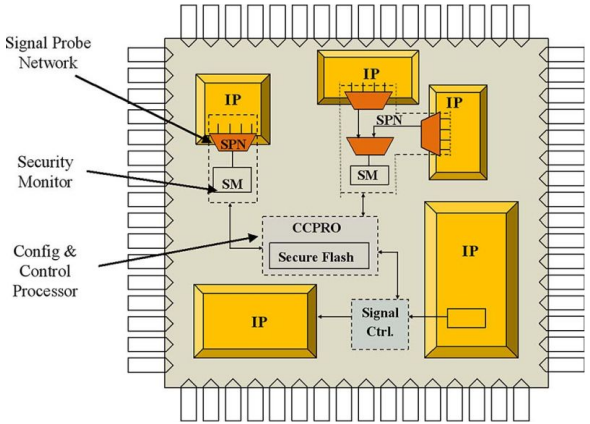
Aly et al., Proc. IEEE, 2019



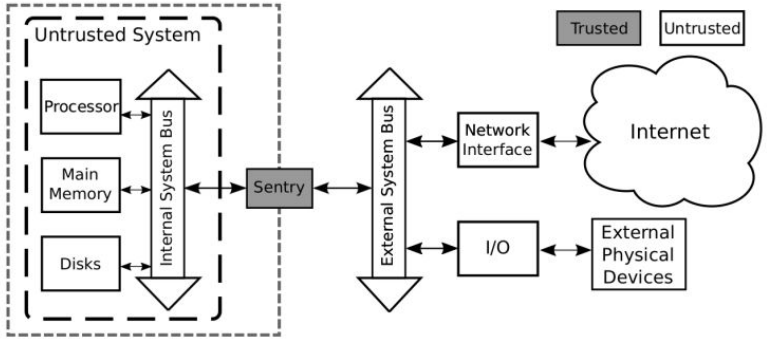
Vivet et al., ISSCC, 2020

Protection of Data

- Internal malicious access/modification: Trojans, design bugs, malicious software
- **Runtime monitoring, dedicated hardware security features**



Bhunia et al., Proc. IEEE, 2014

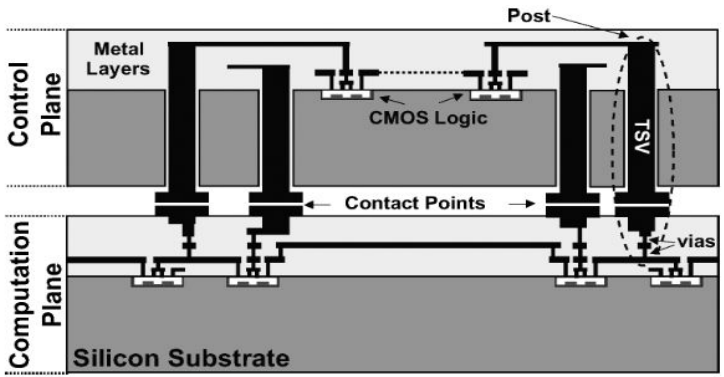


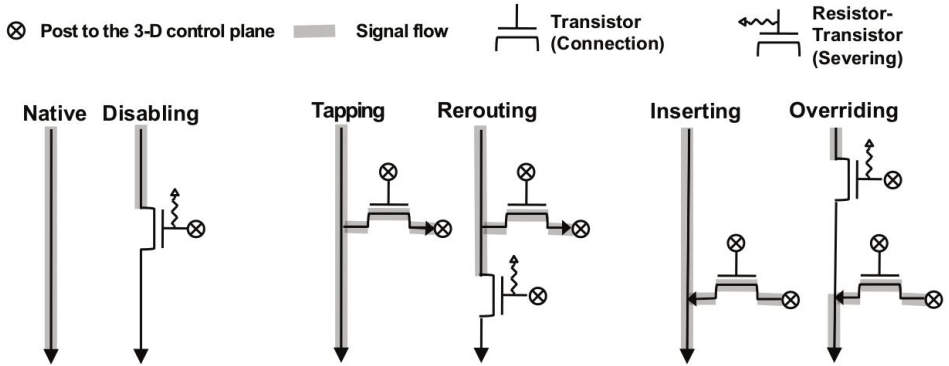
Zhang et al., ASPLOS, 2019

Part I: Exploring the Security Concept

Runtime Monitoring in 2.5D, 3D

- Dedicated hardware security features in 3D



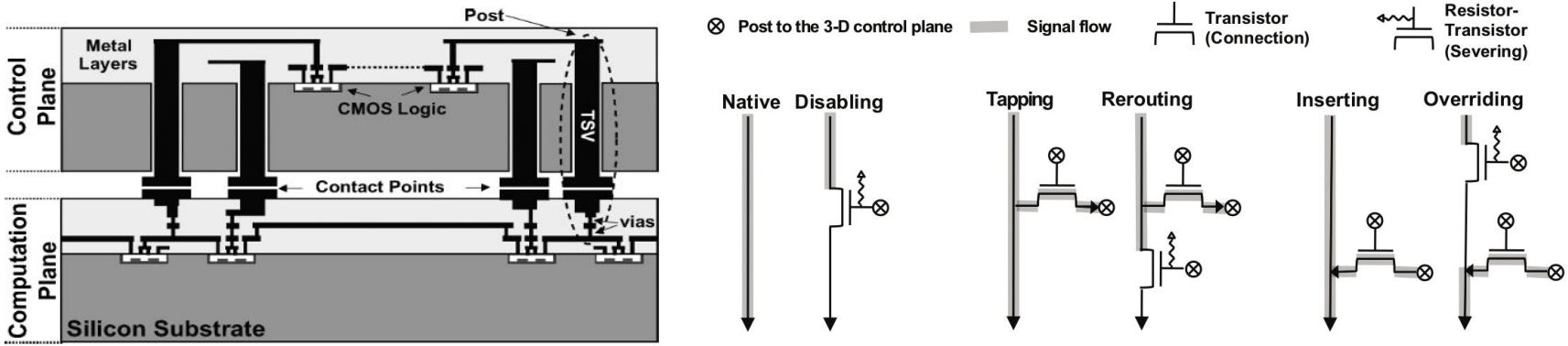


Valamehr et al., ACSAC, 2010

Runtime Monitoring in 2.5D, 3D

- Dedicated hardware security features in 3D
- *But, naïve implementations require trustworthy interfaces from commodity chip – dependency risk*

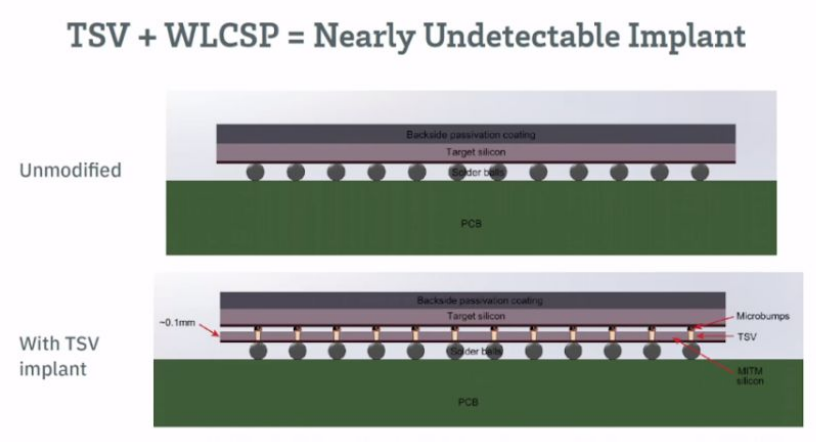
Benefit of 2.5D, 3D Integration: Physical Separation - But Must be Done Right

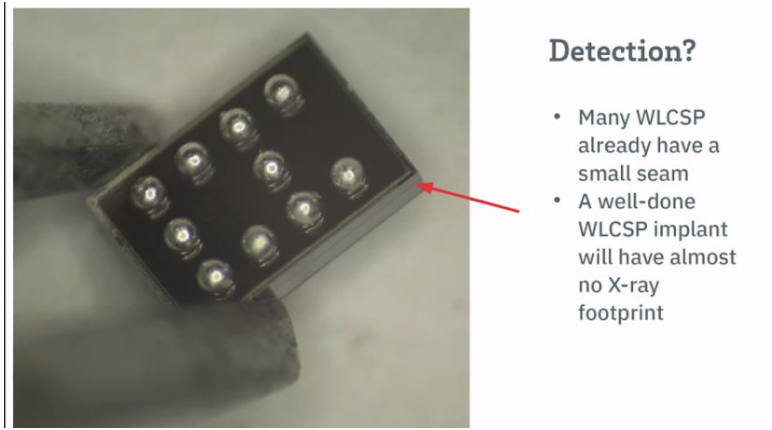


Valamehr et al., ACSAC, 2010

A Note on Supply Chain Threats

- Sneaking in implants between chips in general or security interfaces in particular

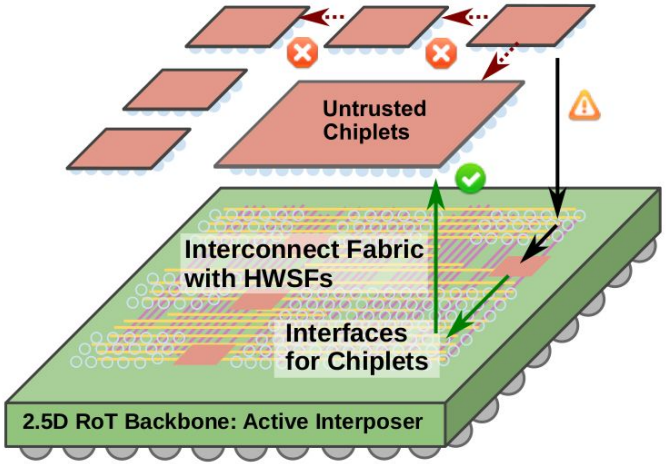


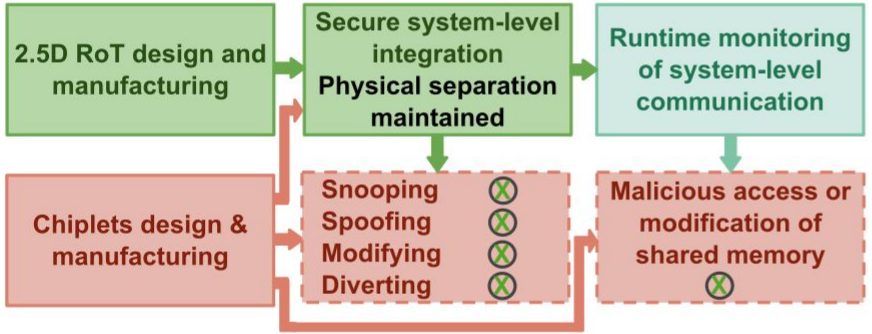


"bunnie" Huang,
36C3, 2019

Physical Separation in 2.5D

- Clear physical separation and support for hardware root of trust
  - No assumptions on untrusted chiplets; may induce any attack on system-level communication
  - Chiplets need to pass all communication through interposer, the secure root of trust backbone
  - (Practical also in stacking-based 3D ICs, but in 2.5D ICs more straightforward)

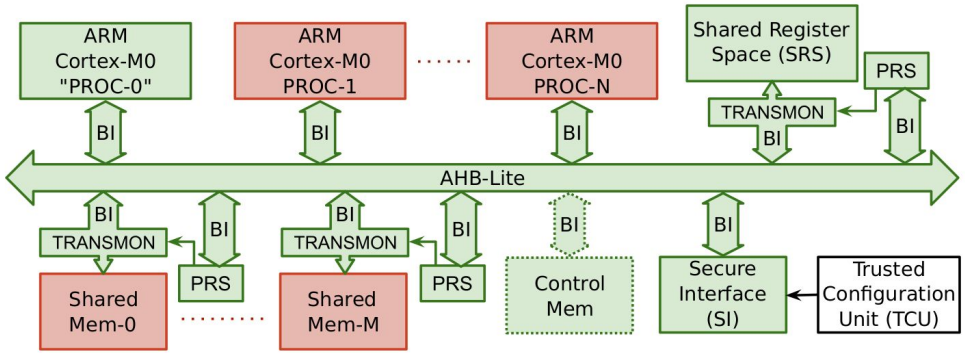


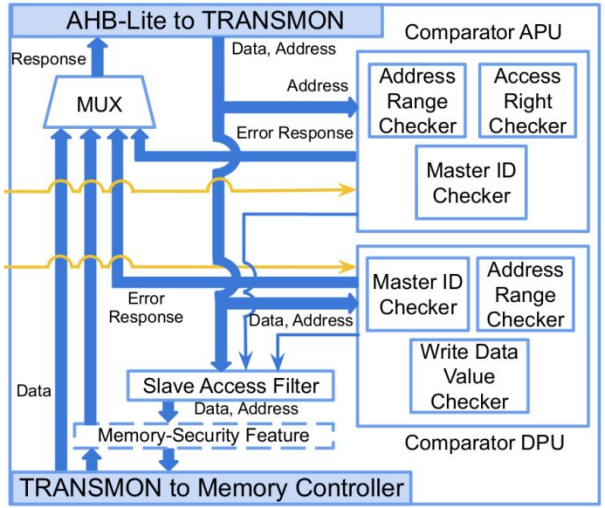


Nabeel et al., TC, 2020

First Case Study

- Overall architecture and root of trust microarchitecture
  - Follows prior art

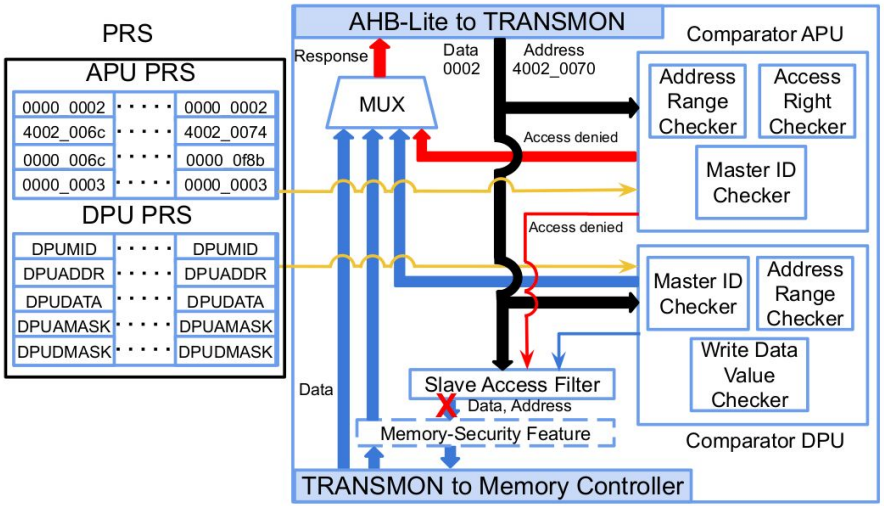




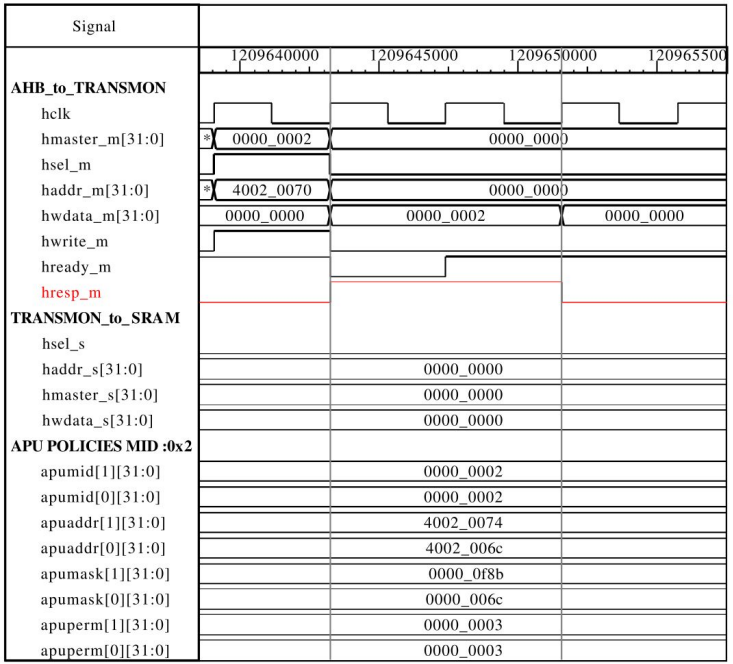
Nabeel et al., TC, 2020

First Case Study

- Security workings
  - Policy checks on memory accesses

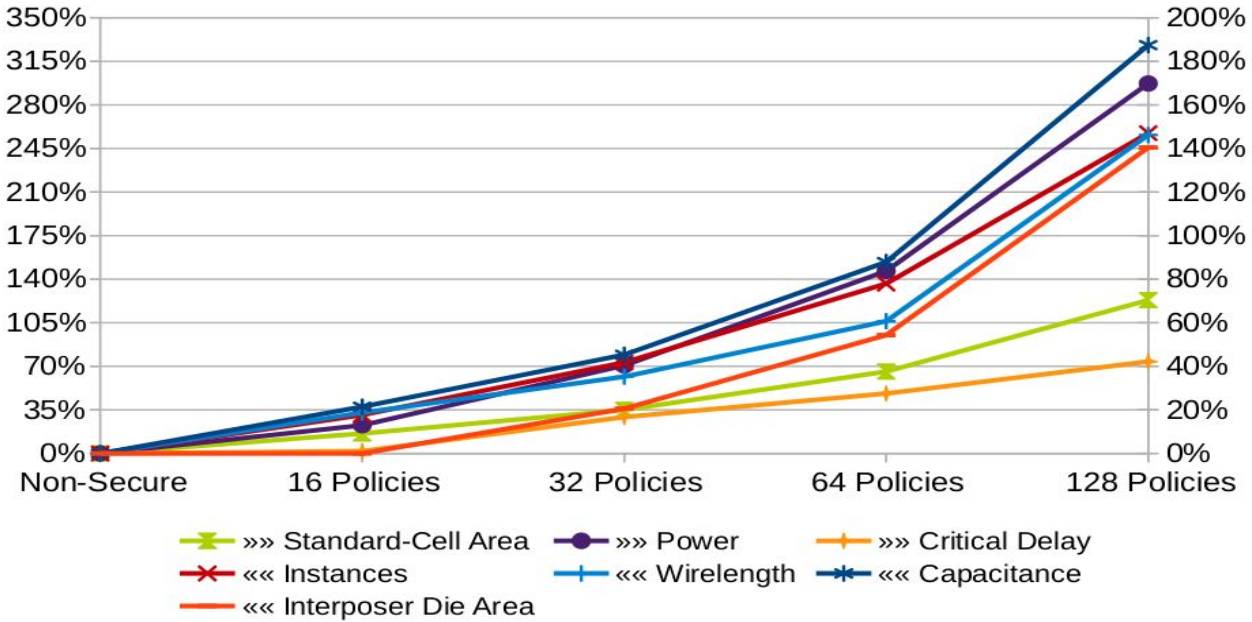


Nabeel et al., TC, 2020



First Case Study

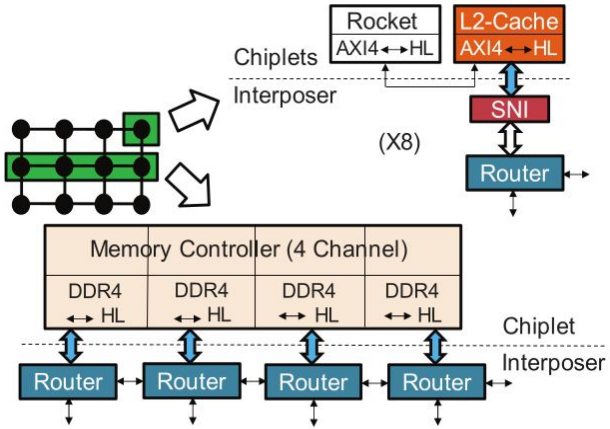
- Implementation overheads

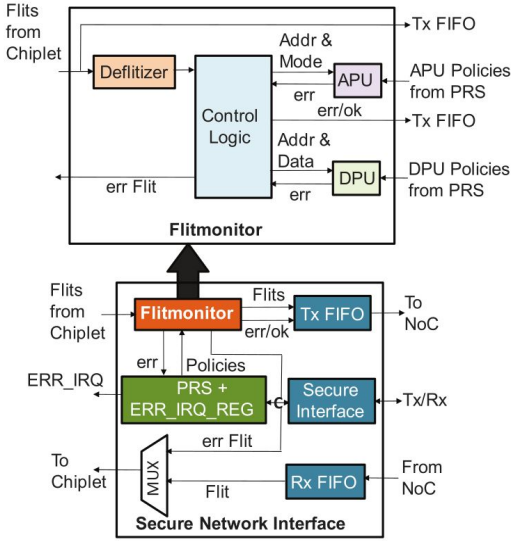


Nabeel et al., TC, 2020

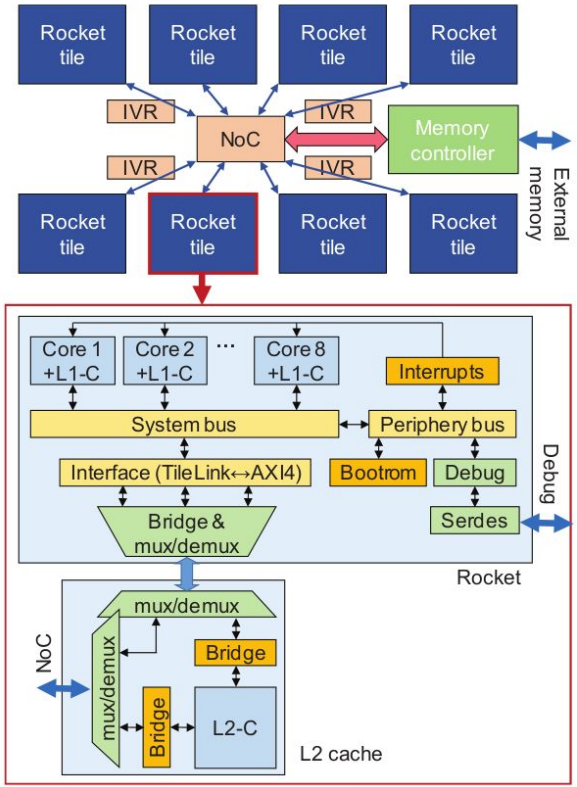
Second Case Study

- Same motivation, principles; <u>study on larger RISC-V system</u>



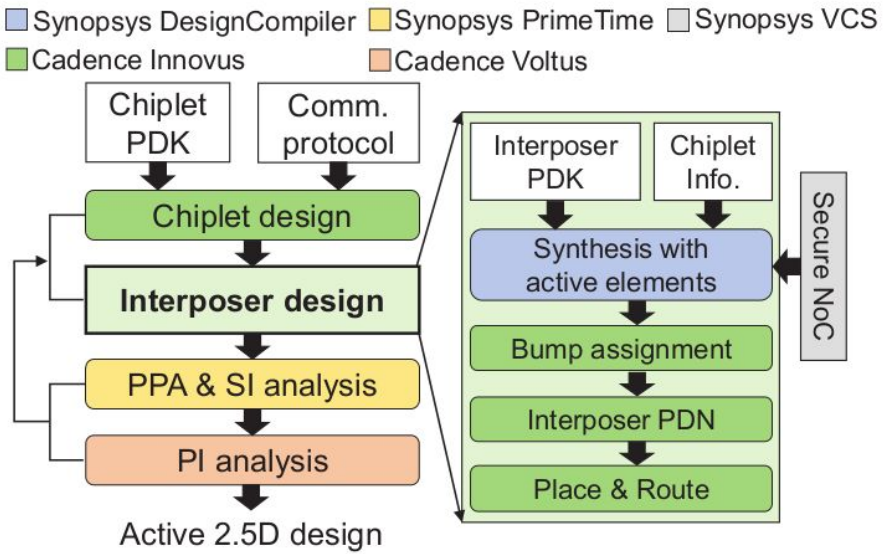


Park et al. TCPMT 2020



Second Case Study

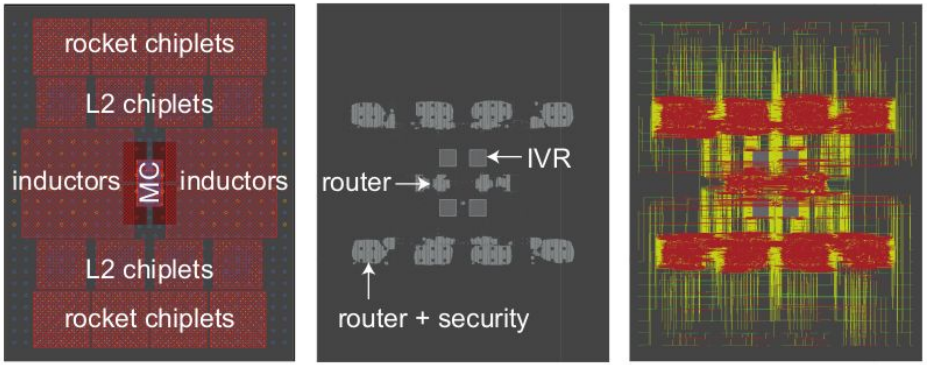
- Industry-grade physical design



Park et al. TCPMT 2020

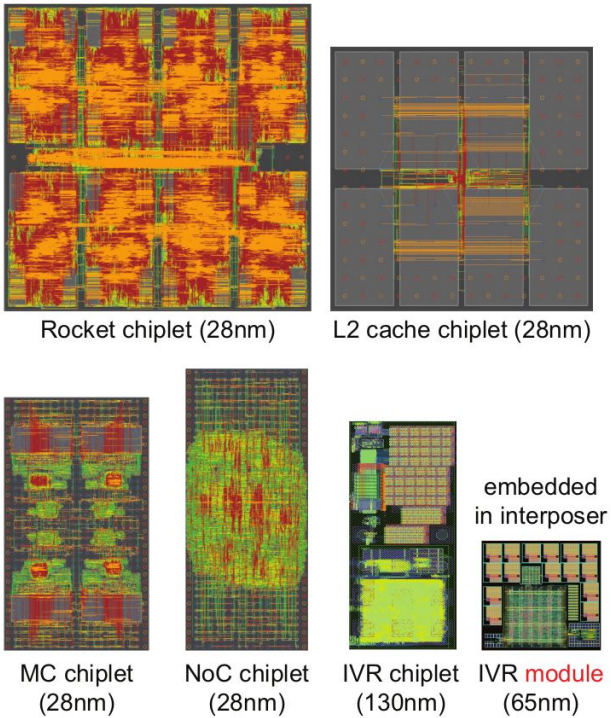
Second Case Study

- Layout snapshots



(c) floorplan (d) interposer placement (e) interposer routing

Park et al. TCPMT 2020



Second Case Study

- Implementation overheads

	Passive	Active
Chiplet Technology	$28nm$, $130nm$	$28nm$
Interposer Technology	$65nm$	$65nm$
Security	Unsecured	Secured
Footprint (mm)	10.8×10.8	8.8×10.8 (-18.5%)
Interposer Cell #	0	480,709
(Repeater #)	(0)	(98,639)
Interposer Utilization	0%	2.68%
# Metal Layers	4	4
Interposer Net #	1,420	481,485
Interposer WL (m)	5.068	30.134 (5.95×)
Avg. Net WL (mm)	3.582 (57.2×)	0.063
Interposer Power	172.8 mW	167.2 mW (-3.2%)
Net Power	172.8 mW	80.2 mW (-53.6%)
Cell Power	-	86.6 mW
Leakage Power	-	0.4 mW

	NoC w/o Security	NoC w/ Security	Cost w.r.t. 2.5D Design
Cell #	132,945	480,709 (3.62×)	+4.56%
Utilization (%)	1.58	2.68	-
Wirelength (m)	11.108	30.134 (2.71×)	+11.83%
Total Power (mW)	66.7	167.2 (2.51×)	+1.17%

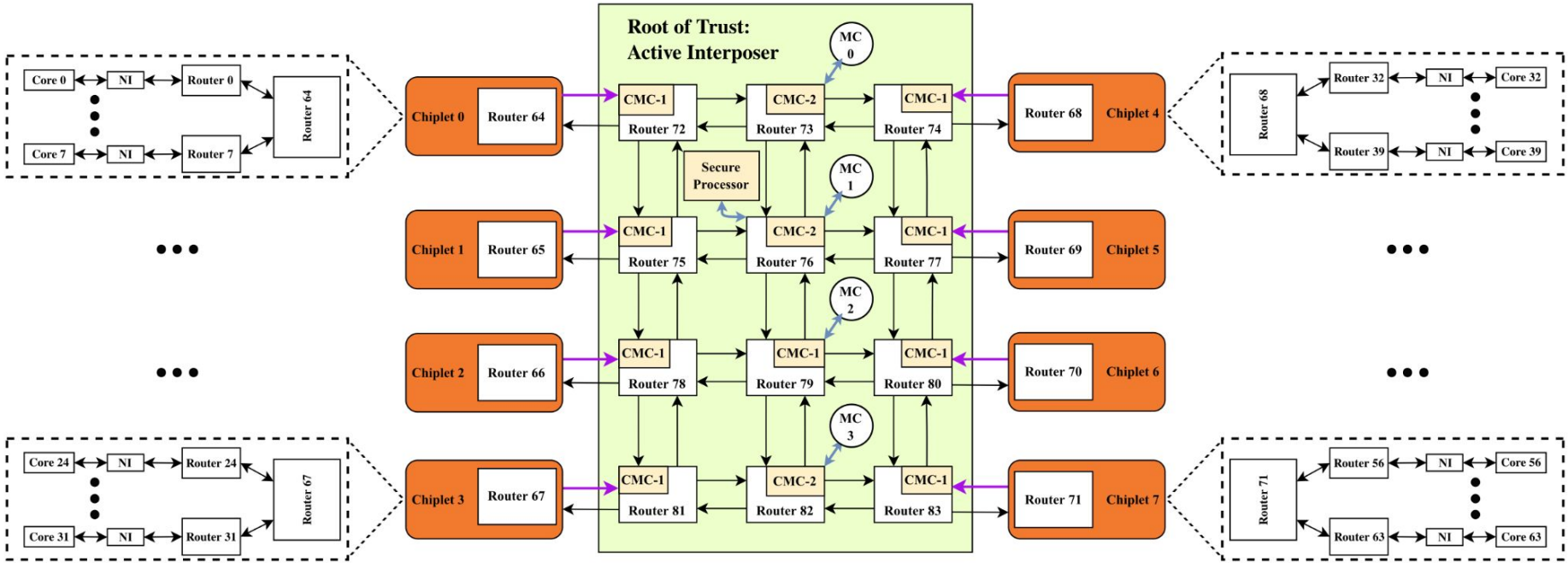
Park et al. TCPMT 2020

جامعة نيويورك أبوظبي
NYU | ABU DHABI
CENTER FOR CYBER SECURITY
DFX LAB
DESIGN FOR EXCELLENCE

Part II: Trojan Threats on Coherence in 2.5D Systems

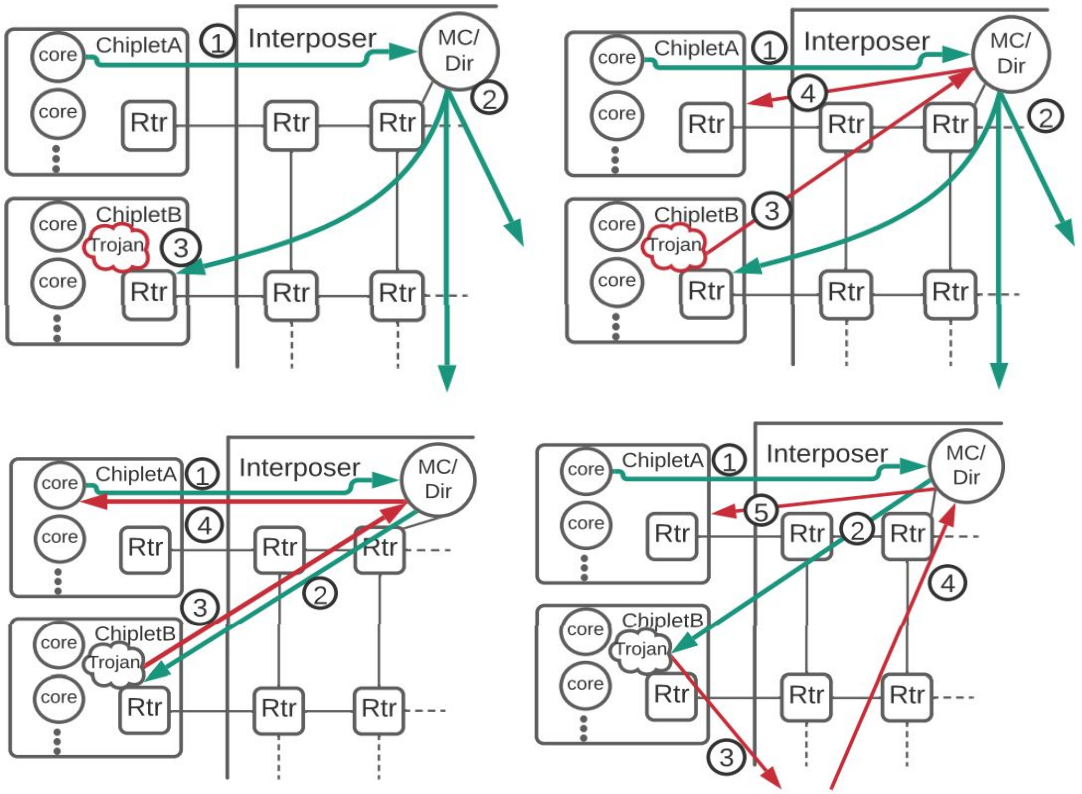
Third Case Study

- Same motivation, principles; study on larger RISC-V system; study on cache coherence
  - System-level emulation using gem5 and SPEC benchmarks, not on RTL



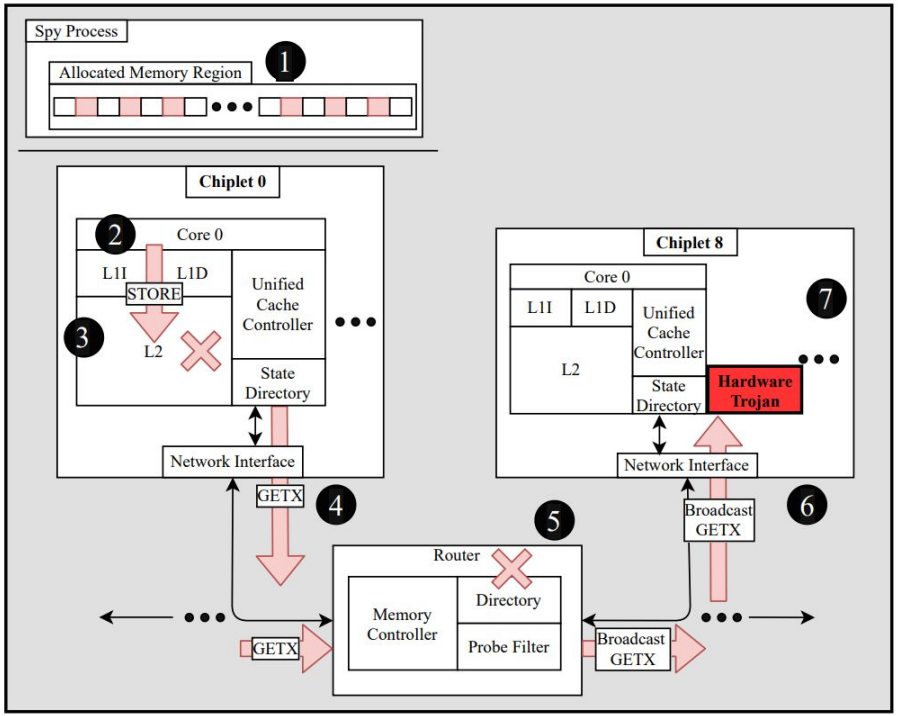
Third Case Study

- Four different Trojan scenarios (top to bottom, left to right):
  - Snooping
  - Spoofing
  - Modifying
  - Diverting



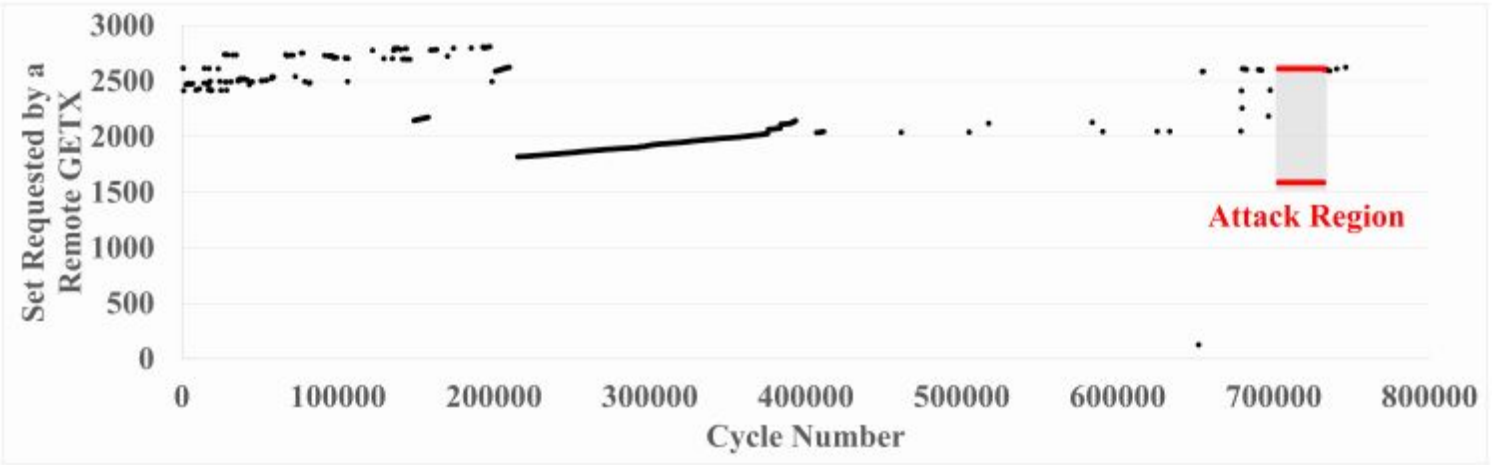
Third Case Study

- An orchestrated attack: data leaked via covert channel across chiplets
  - Receiver chiplet has no access to address range, but Trojan (or receiver process)
  - Actions legal within coherence protocol; vulnerability comes from GETX broadcast to all cores



Third Case Study

- An orchestrated attack: data leaked via covert channel across chiplets
  - Receiver chiplet has no access to address range
  - Actions legal within coherence protocol; vulnerability comes from GETX broadcast to all cores
  - **Bits 0, 1 to leak are encoded as addresses, which are requested through coherence directory**

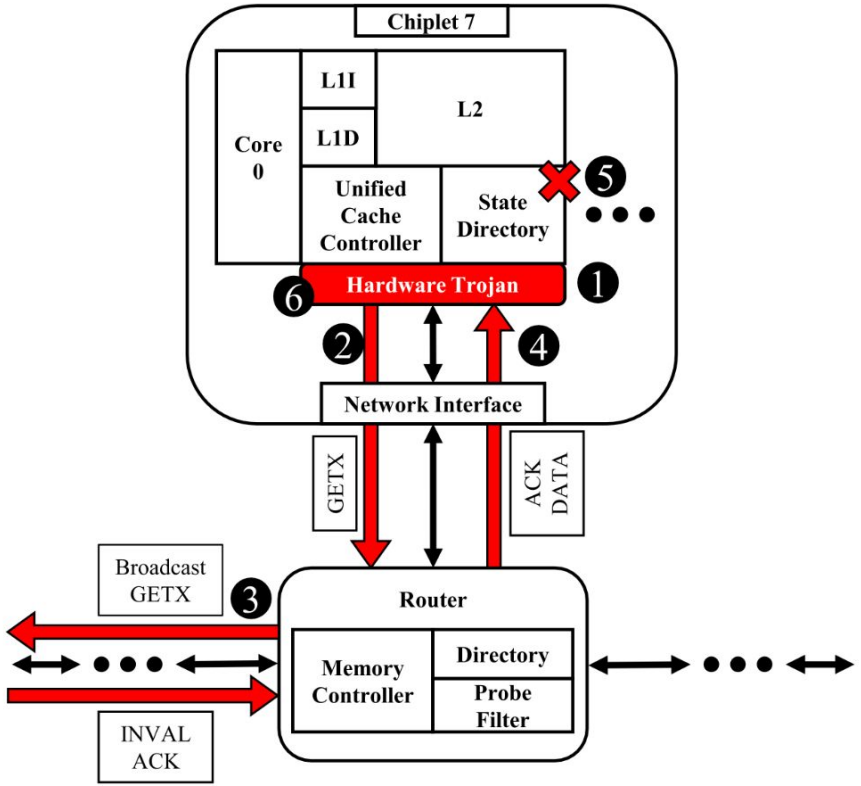


Third Case Study

- Another orchestrated attack: forging to gain control and modify other chiplets' data
  - Setting: Trojan-compromised chiplet
    - does not have access to the victim's address space,
    - has never held target data in its caches,
    - does not interact with the victim in any way during execution

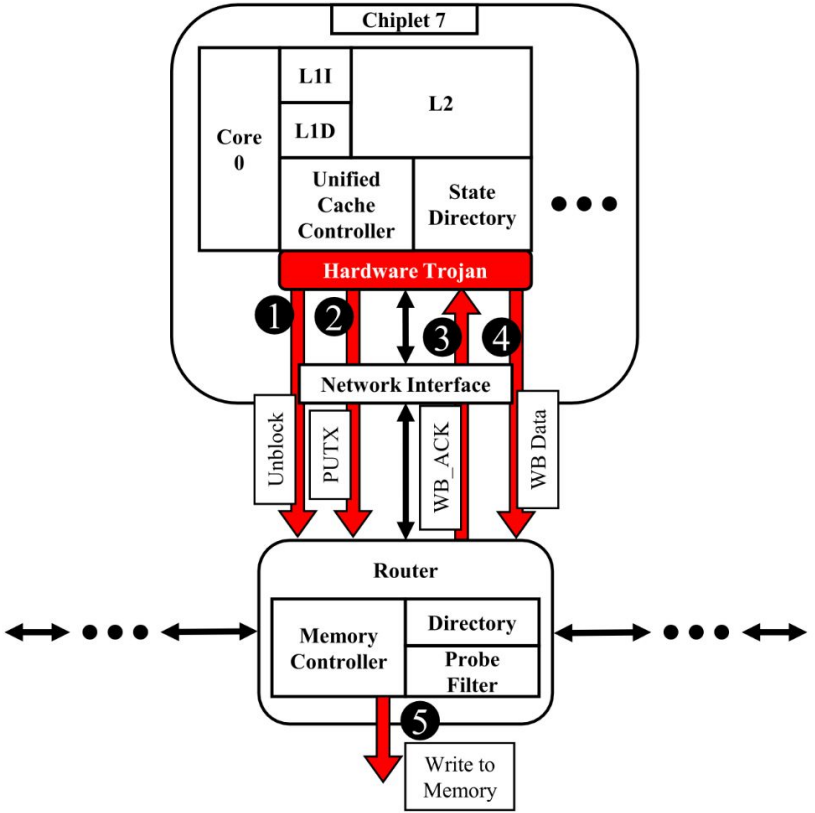
Third Case Study

- Another orchestrated attack: forging to gain control and modify other chiplets' data
  - Setting: Trojan-compromised chiplet
    - does not have access to the victim's address space,
    - has never held target data in its caches,
    - does not interact with the victim in any way during execution
  - **Phase 1: Trojans gains control of target address range, unknown to core / OS**



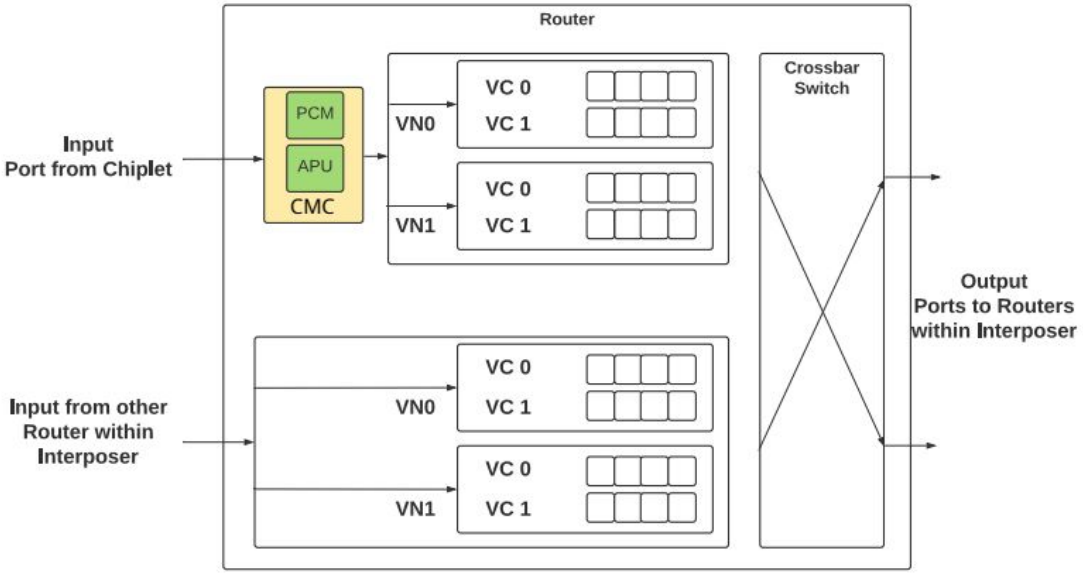
Third Case Study

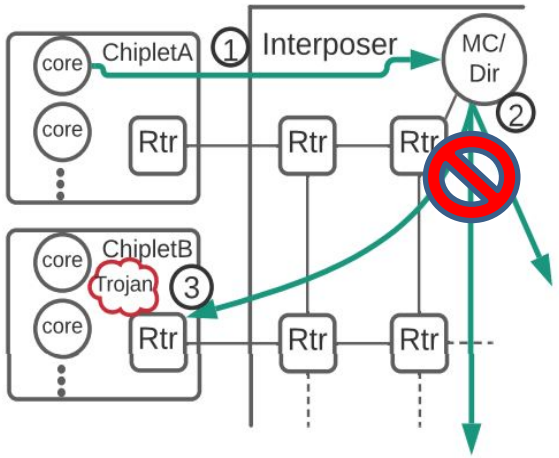
- Another orchestrated attack: forging to gain control and modify other chiplets' data
  - Setting: Trojan-compromised chiplet
    - does not have access to the victim's address space,
    - has never held target data in its caches,
    - does not interact with the victim in any way during execution
  - Phase 1: Trojans gains control of target address range, unknown to core / OS
  - **Phase 2: Write back malicious data, evicting back to main memory**



Third Case Study

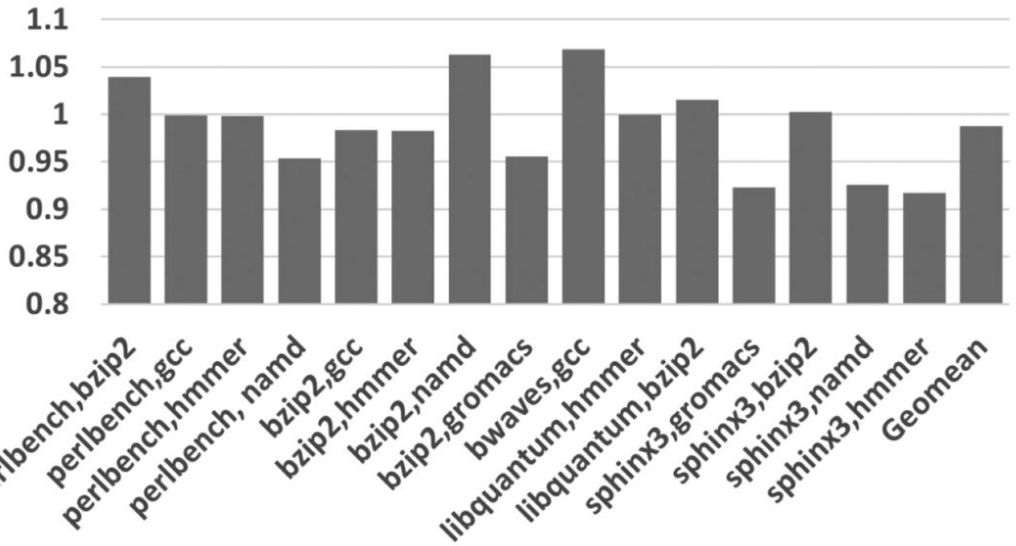
- Security concept: policy checking and, e.g., rewriting GETX
  - **Orchestrated attacks prevented by blocking their underlying basic attacks**





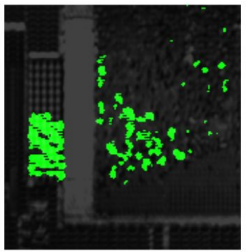
Third Case Study

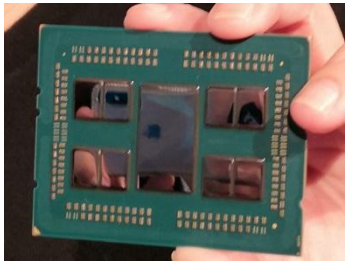
- Performance, in terms of latency
  - Simple policy approvals for some; marginal impact
  - Cache misses for others; larger impact since rewriting is more complex
  - Speedup due to filtering of broadcasts

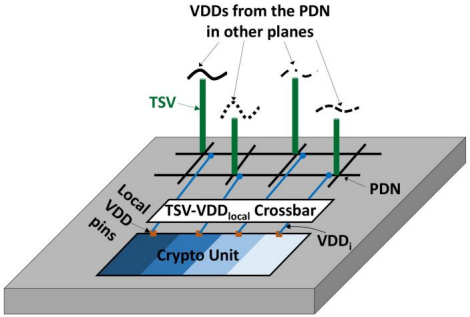


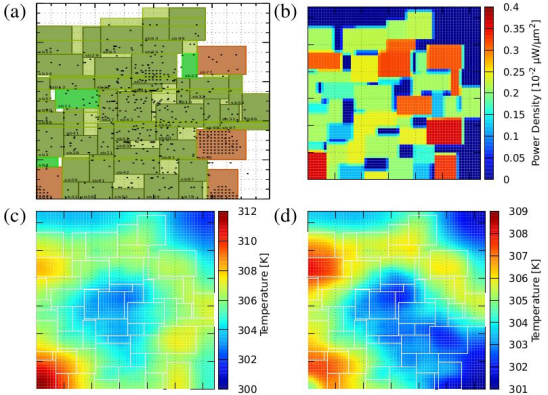
Conclusion

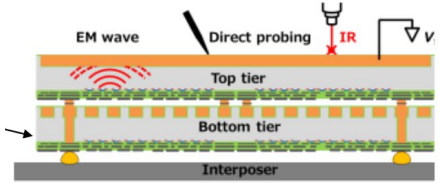
- 3D integration: up and coming, “More Moore” and “More than Moore”
- Physical separation, variability, tampering resilience for security
- But, more complex designs; threats like Trojans more severe

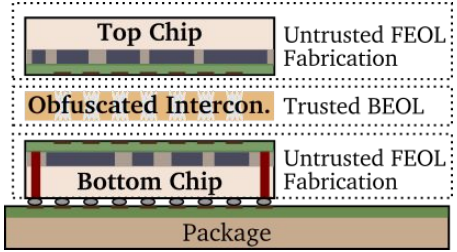


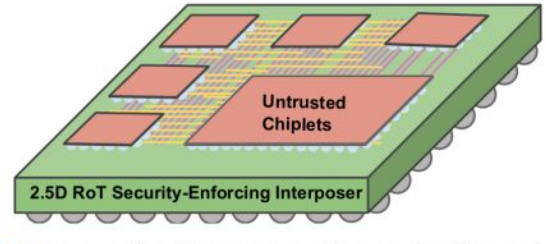












References

- Knechtel et al. On Mitigation of Side-Channel Attacks in 3D ICs: Decorrelating Thermal Patterns from Power and Activity Proc. ACM Des. Autom. Conf. (DAC), 2017, 12:1-12:6
- Patnaik et al. Best of Both Worlds: Integration of Split Manufacturing and Camouflaging into a Security-Driven CAD Flow for 3D ICs Proc. IEEE/ACM Int. Conf. Comput.-Aided Des. (ICCAD), 2018, 8:1-8:8
- Knechtel et al. 3D Integration: Another Dimension Toward Hardware Security Proc. IEEE Int. On-Line Test Symp. (IOLTS), 2019
- Johann Knechtel, Ozgur Sinanoglu, Ibrahim Abe M. Elfadel, Jens Lienig, Cliff C. N. Sze: Large-Scale 3D Chips: Challenges and Solutions for Design Automation, Testing, and Trustworthy Integration. IPSJ Trans. Syst. LSI Des. Methodol. 10: 45-62 (2017)
- Patnaik et al. A Modern Approach to IP Protection and Trojan Prevention: Split Manufacturing for 3D ICs and Obfuscation of Vertical Interconnects IEEE Trans. Emerg. Topics Comput. (TETC), 2019
- Rangarajan et al. The Next Era in Hardware Security, Springer 2021
- Park et al. Design Flow for Active Interposer-Based 2.5D ICs and Study of RISC-V Architecture with Secure NoC IEEE Trans. Compon., Pack., Manuf. Tech. (TCPMT), 2020, 10, 2047-2060
- Nabeel et al. 2.5D Root of Trust: Secure System-Level Integration of Untrusted Chiplets IEEE Trans. Comput. (TC), 2020, 69, 1611-1625
- Gino A. Chacon, Charles Williams, Johann Knechtel, Ozgur Sinanoglu, Paul V. Gratz:Hardware Trojan Threats to Cache Coherence in Modern 2.5D Chiplet Systems. IEEE Comput. Archit. Lett. 21(2): 133-136 (2022)
- Gino A. Chacon, Charles Williams, Johann Knechtel, Ozgur Sinanoglu, Paul V. Gratz, Vassos Soteriou: Coherence Attacks and Countermeasures in Interposer-based Chiplet Systems. ACM Trans. Archit. Code Optim. 21(2): 23 (2024)