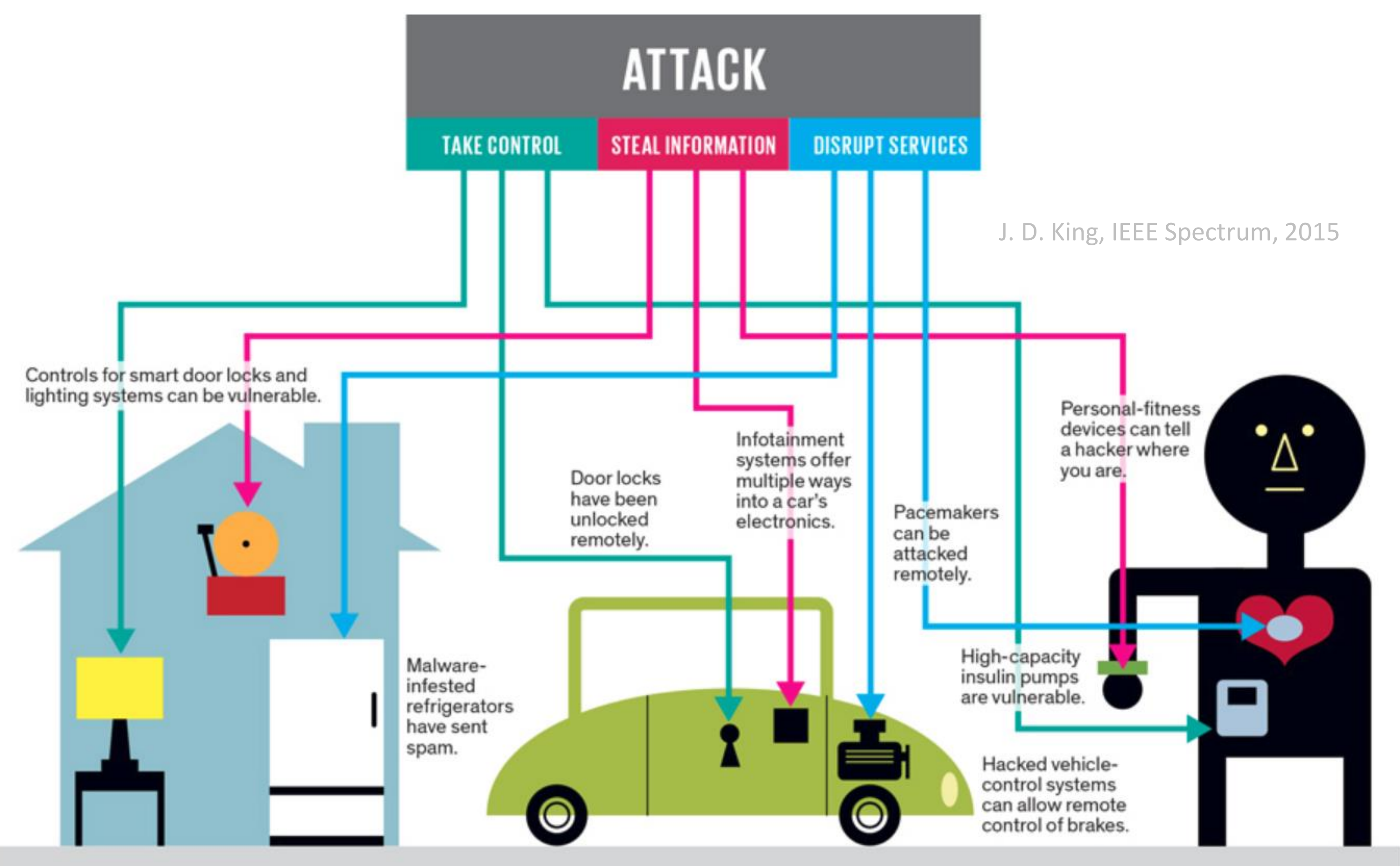
جامعة نيويورك أبوظبي
NYU | ABU DHABI

3D Integration: Another Dimension Toward Hardware Security

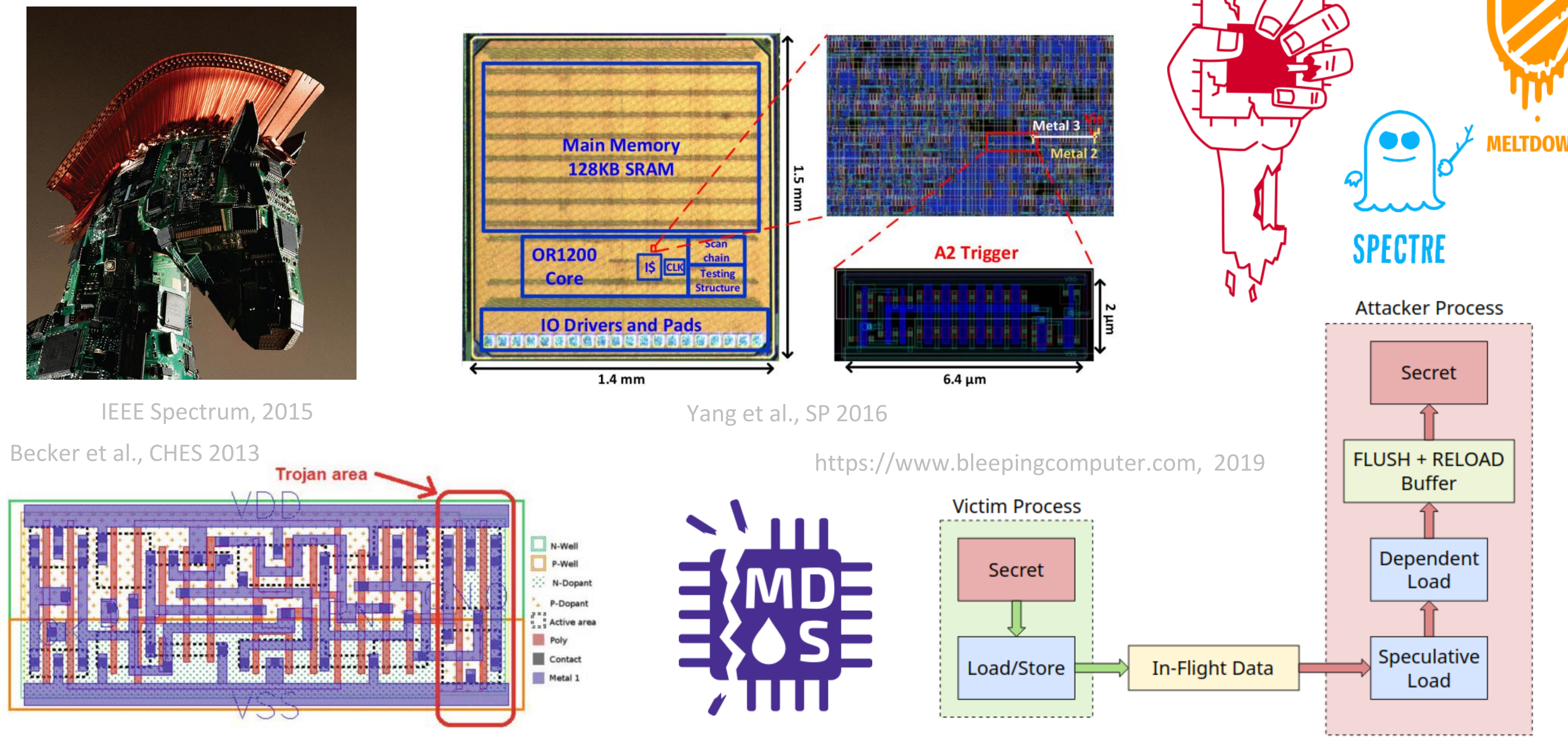
Johann Knechtel, Satwik Patnaik, and Ozgur Sinanoglu
{johann, sp4012, ozgursin}@nyu.edu

IOLTS 2019, July 2, Rhodes, Greece



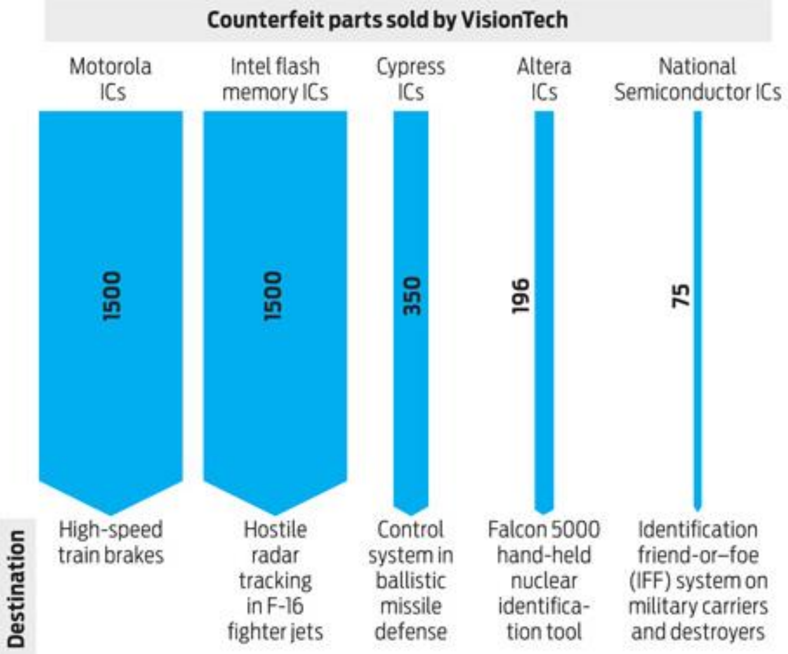
J. D. King, IEEE Spectrum, 2015

Data and Computation at Risk – Right at the Hardware



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

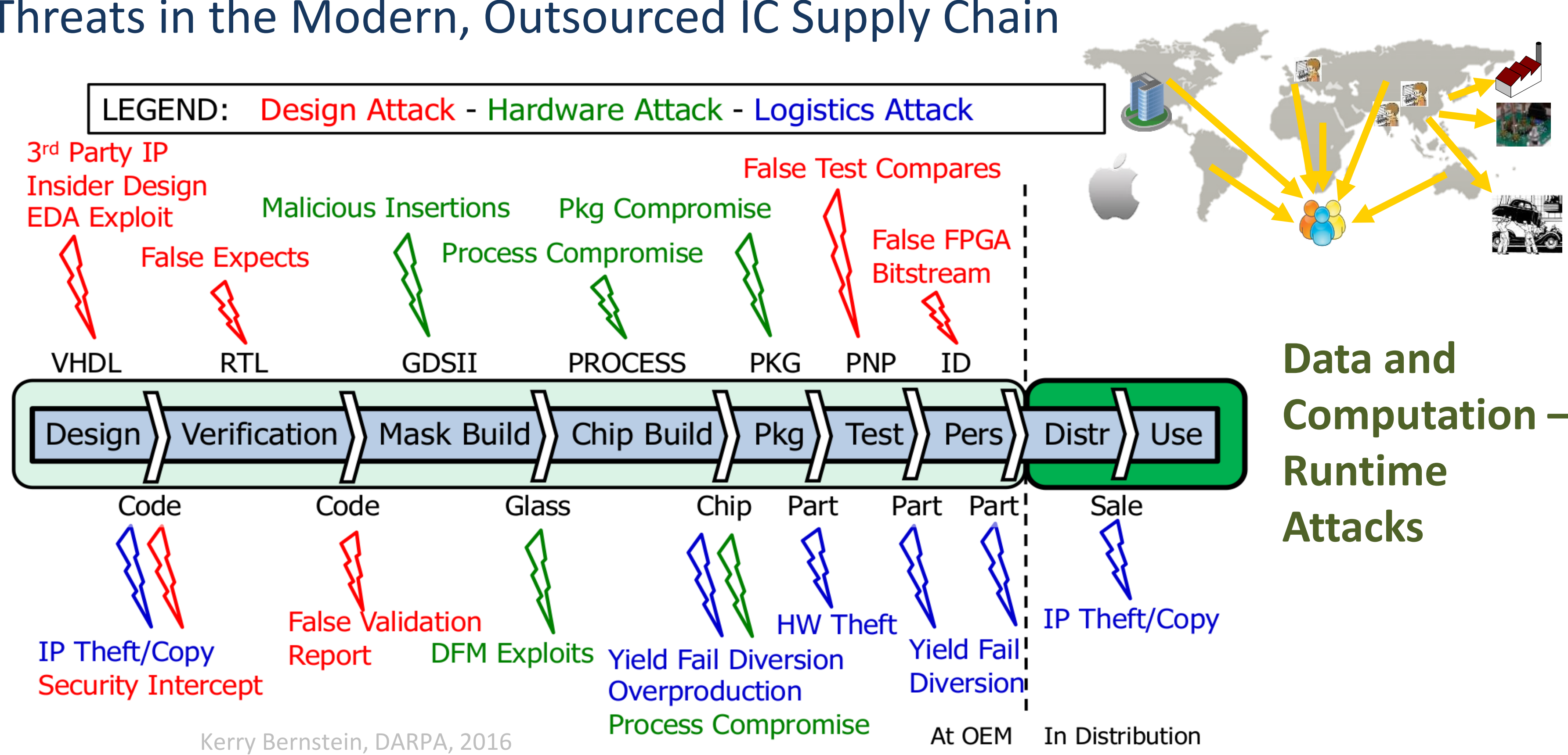
Hardware Itself Also at Risk



APRIL 2019: ZHENGZHOU CUSTOMS DESTROYS COUNTERFEIT TI CHIPS WORTH 704M YUAN

Zhengzhou Customs seized 20,000 automotive CPU ICs labeled with the Texas Instruments (TI) trademark, suspecting them to be counterfeit. […] Total value of the fake chips was estimated at 704 million yuan. (around 100 million USD).

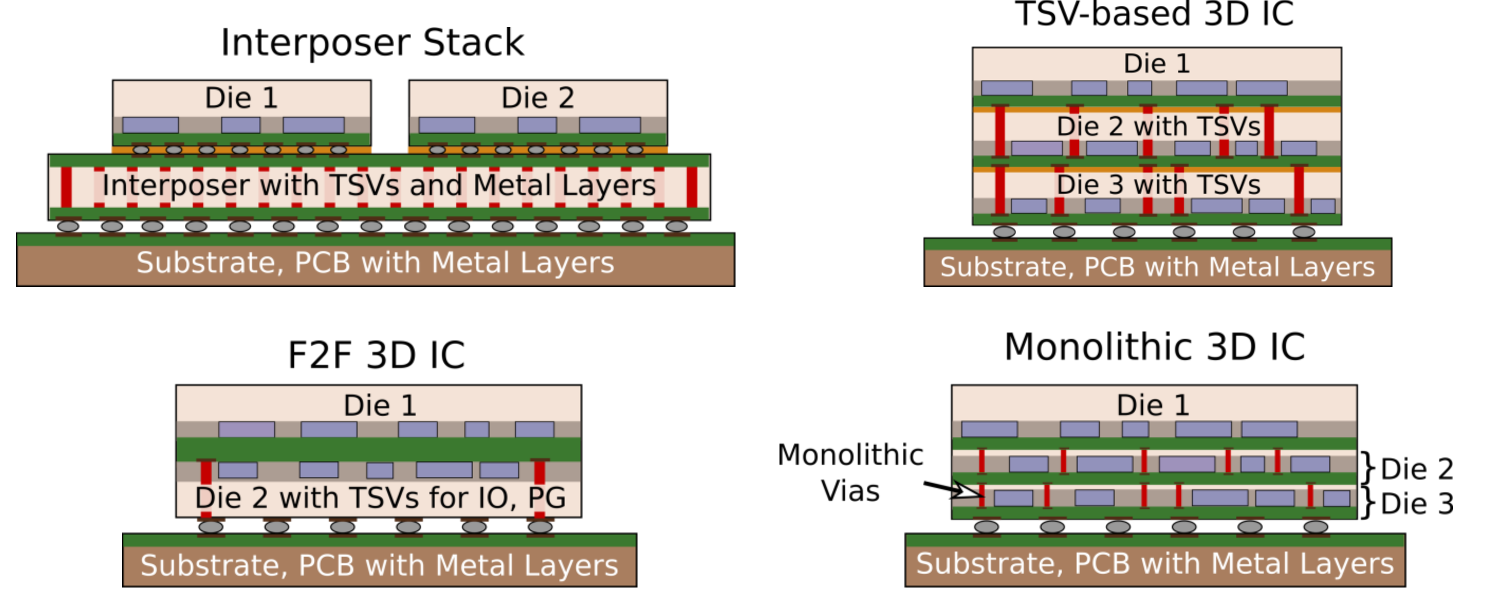
Threats in the Modern, Outsourced IC Supply Chain



Data and Computation – Runtime Attacks

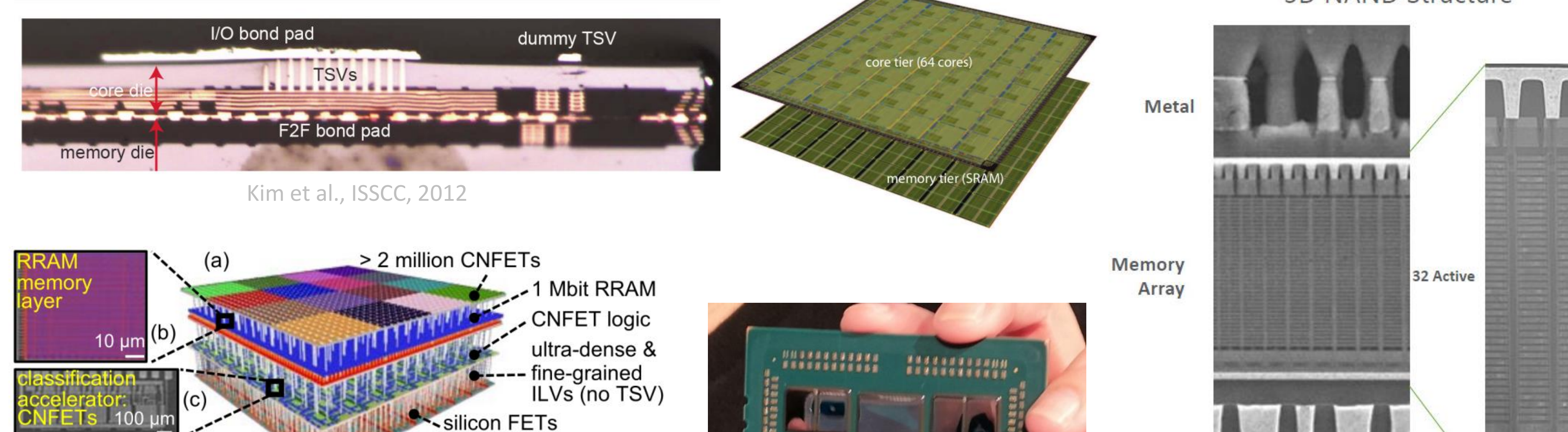
3D Integration: Stacking and Interconnection of Chips

- Shorter, vertical interconnects: power consumption, delay, bandwidth – "More Moore"
- Separate dies: heterogeneous and larger systems, yield, **security** – "More than Moore"
- More complex design, design automation, and manufacturing processes



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

3D Integration: Stacking and Interconnection of Chips



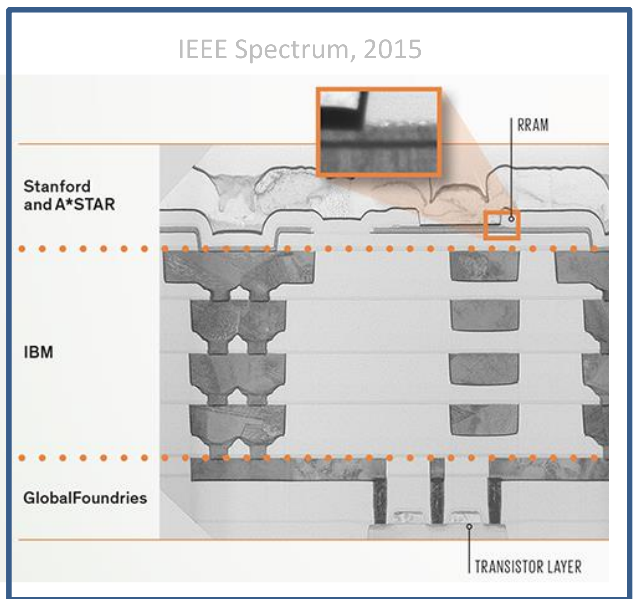
Kim et al., ISSCC, 2012

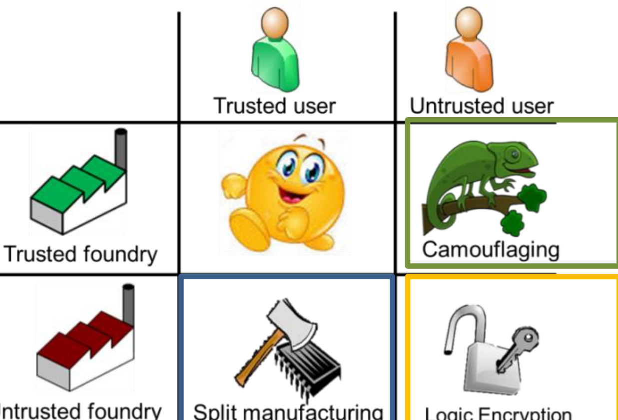
Aly et al., Proc. IEEE, 2019

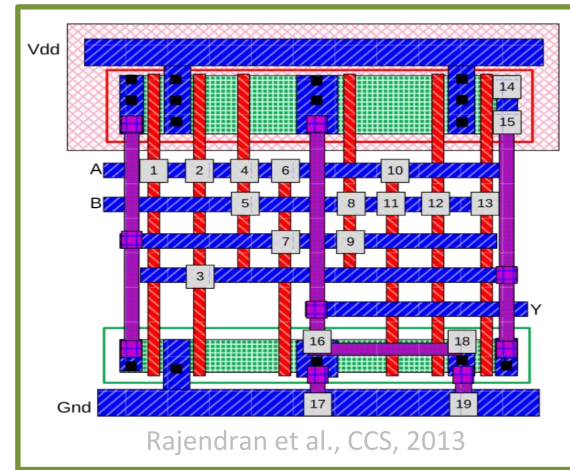
https://www.anandtech.com, 2016 & 2018

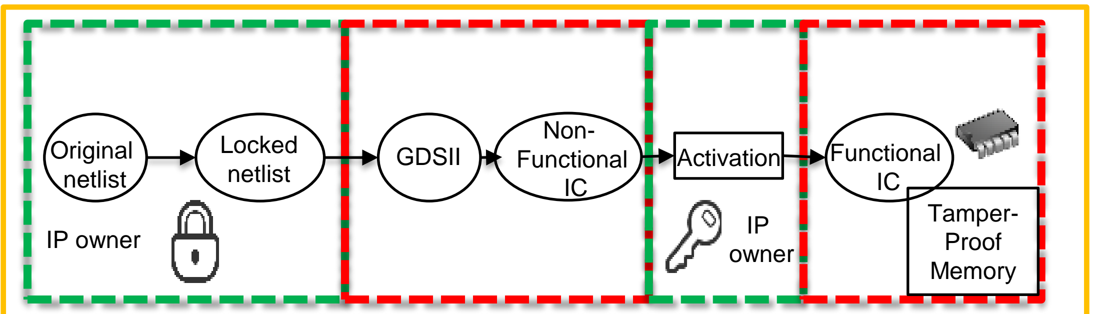
Protection of Design IP – An Overview

Benefit of 3D Integration: Physical Separation





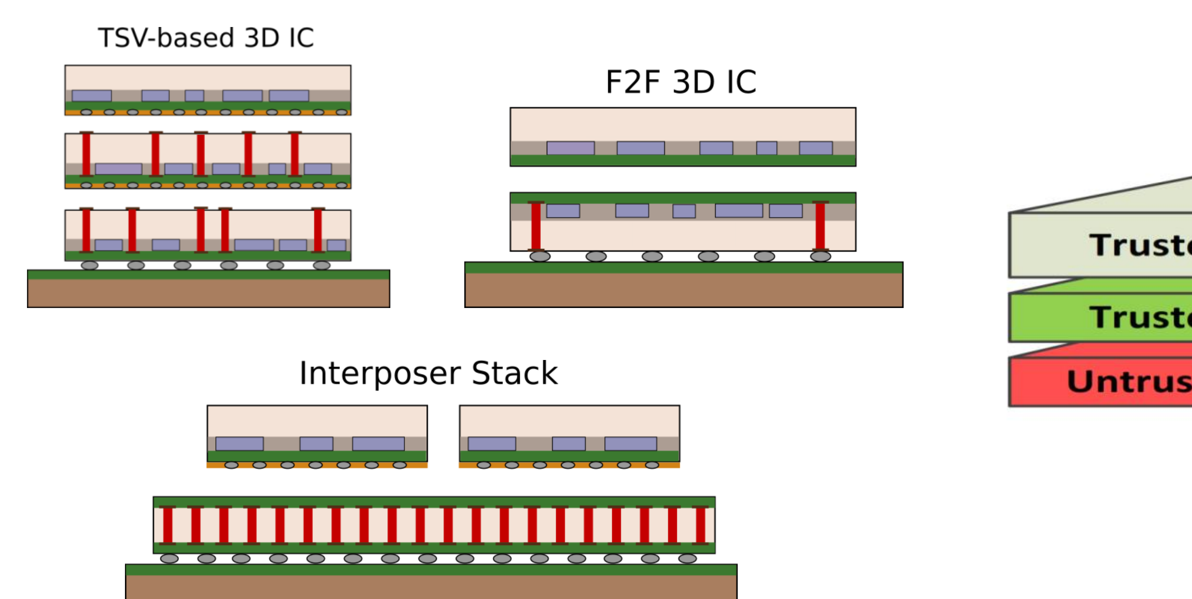


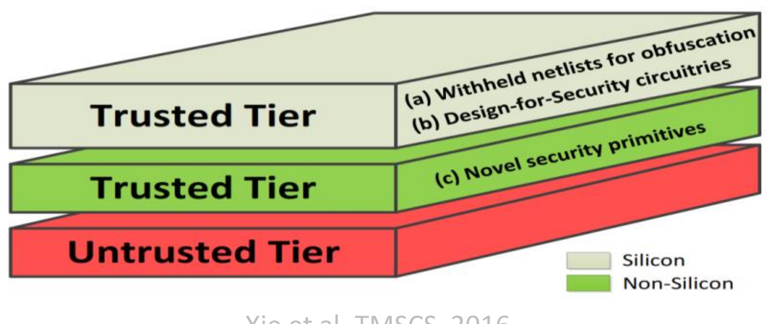


Knechtel et al., 3D Integration: Another Dimension Towards Hardware Security, IOLTS 2019

Split Manufacturing in 3D Integration – A Natural Match

- Physical separation into trusted and untrusted parts
- More flexible: system-level splitting into multiple dies
- More practical: FEOL and BEOL processing uninterrupted (except for monolithic 3D)



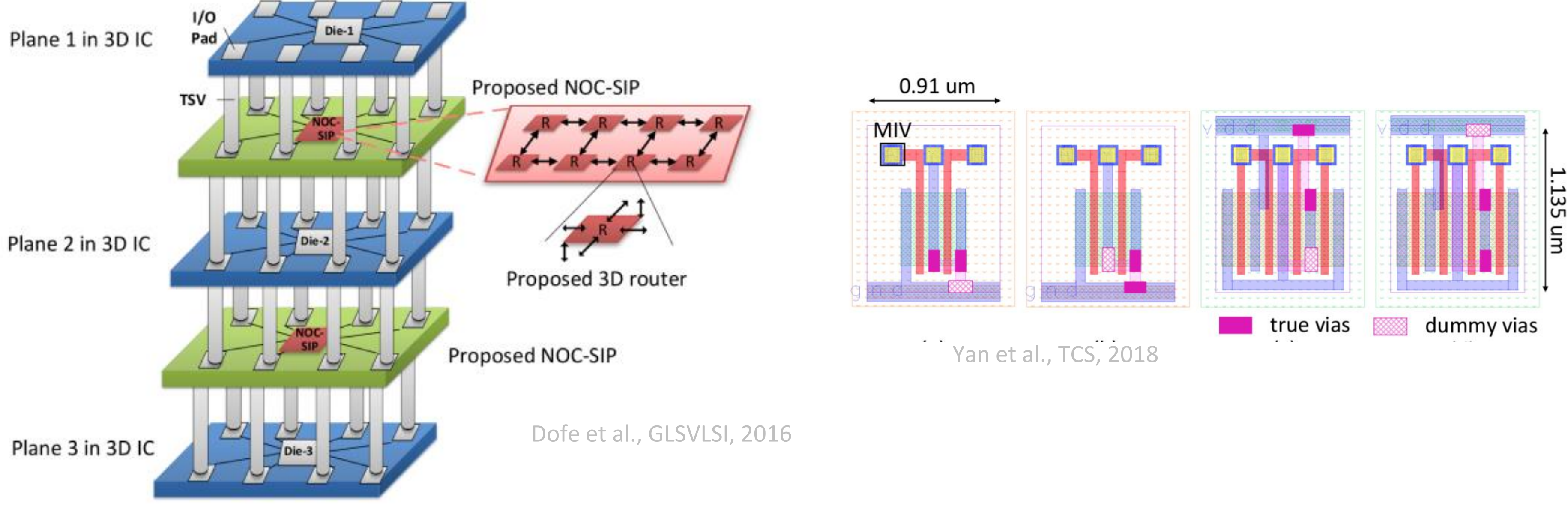


Xie et al.,TMSCS, 2016

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

Examples for Split Manufacturing, Camouflaging in 3D

- Split manufacturing of 3D NoC: flexible, generic, obfuscation of system-level interconnects
- Camouflaging of monolithic 3D cells: superior layout cost than 2D camouflaging

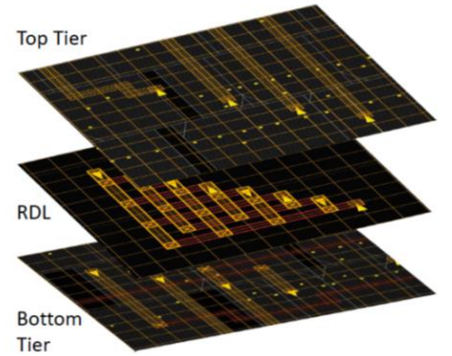


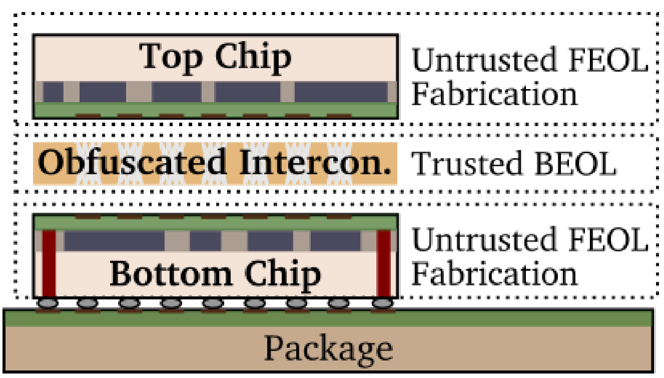
Dofe et al., GLSVLSI, 2016

Yan et al., TCS, 2018

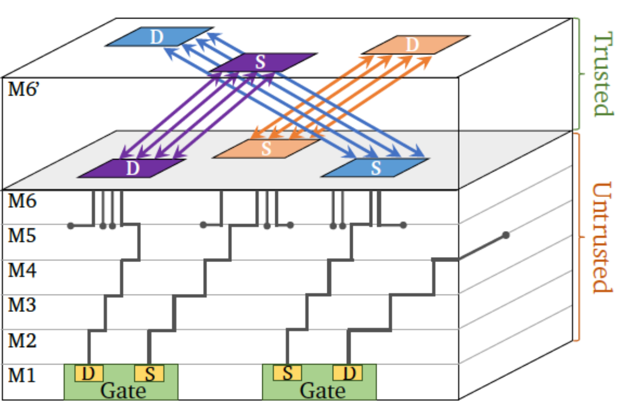
Split Manufacturing **and** Camouflaging in 3D – “Best of Both Worlds”

- Prior art: high cost, protect only against fab or end-user
- Obfuscate vertical interconnects (RDLs)
- Only trusted BEOL and resilient BEOL materials required
- Thwarts both malicious foundries <u>and</u> end-user
- Reasonable layout cost



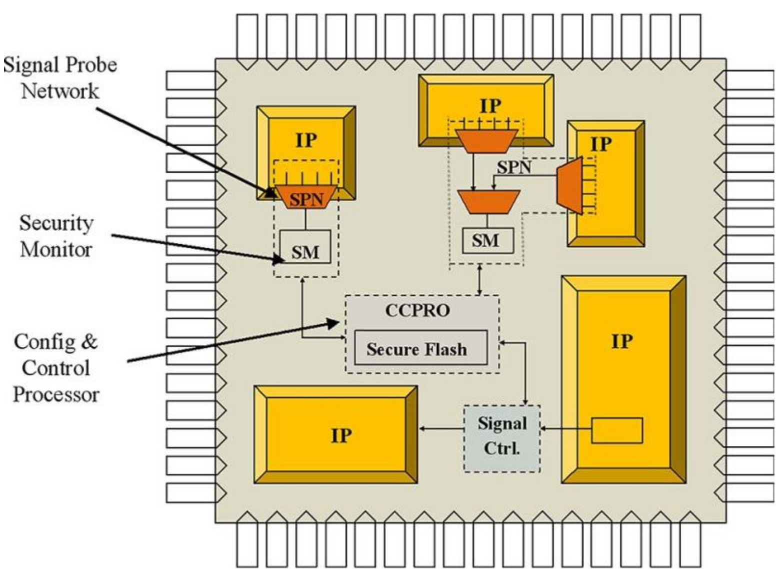


Patnaik et al., ICCAD, 2018

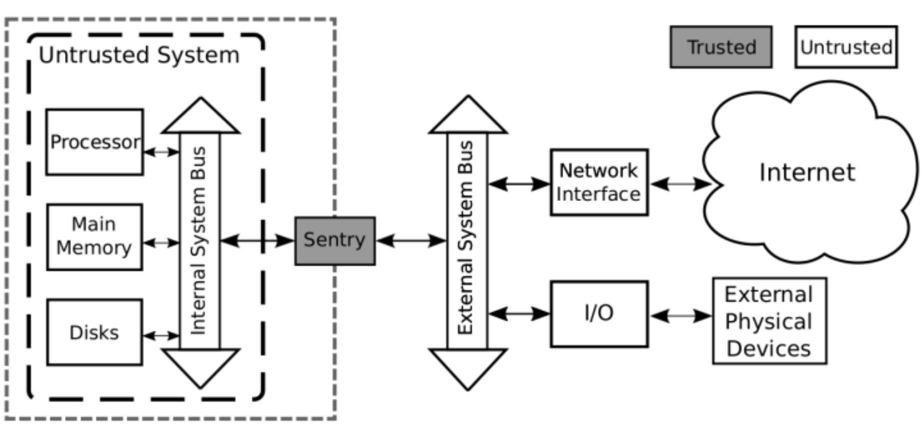


Protection of Data and Computation (1)

- ⚠ (1) Internal access/modification: Trojans, design bugs, malicious software
- ➡ Monitoring at runtime, dedicated hardware security features



Bhunia et al., Proc. IEEE, 2014

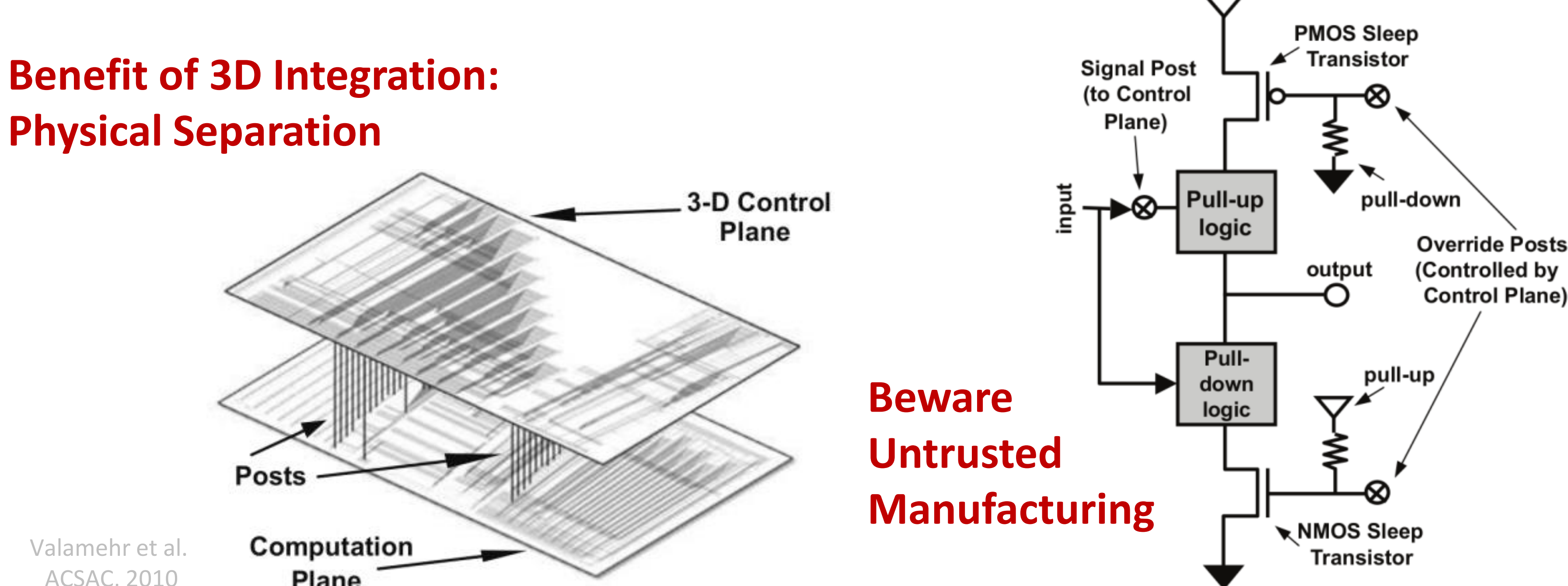


Zhang et al., ASPLOS, 2019

Protection of Data and Computation (1) **in 3D**

- (1) Internal access/modification: Trojans, design bugs, malicious software
- Monitoring at runtime, dedicated hardware security features

Benefit of 3D Integration: Physical Separation



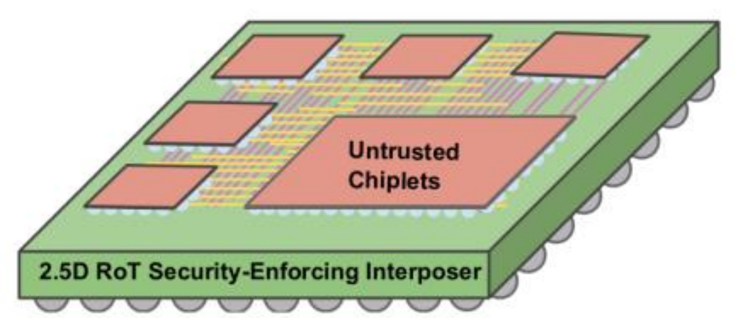
Beware Untrusted Manufacturing

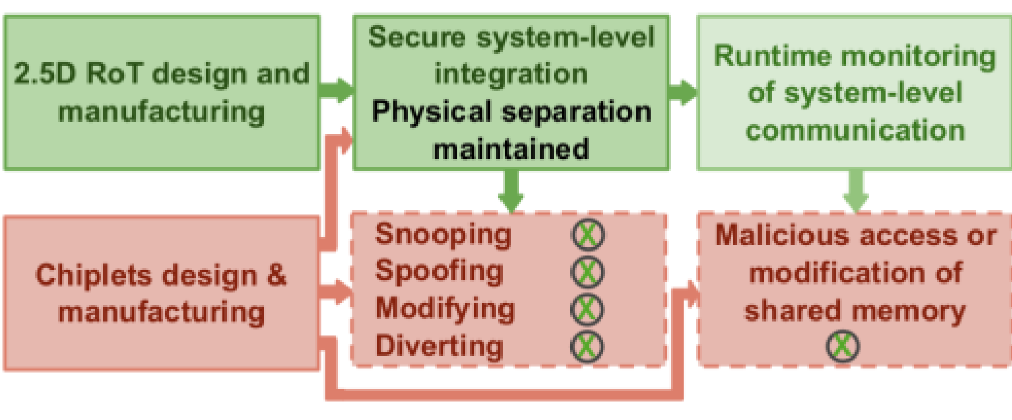
Knechtel et al., 3D Integration: Another Dimension Towards Hardware Security, IOLTS 2019

Protection of Data and Computation (1) **in 2.5D**

- (1) Internal access/modification: Trojans, design bugs, malicious software
- Monitoring at runtime, dedicated hardware security features – fully separated root of trust

Benefit of 3D/2.5D Integration: Physical Separation

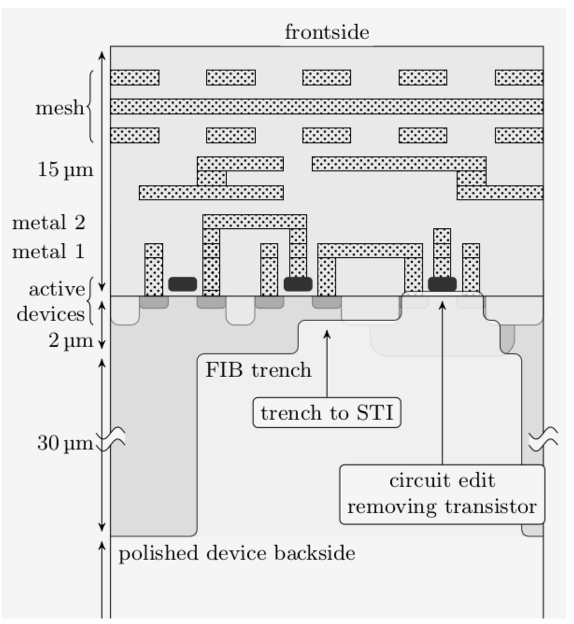




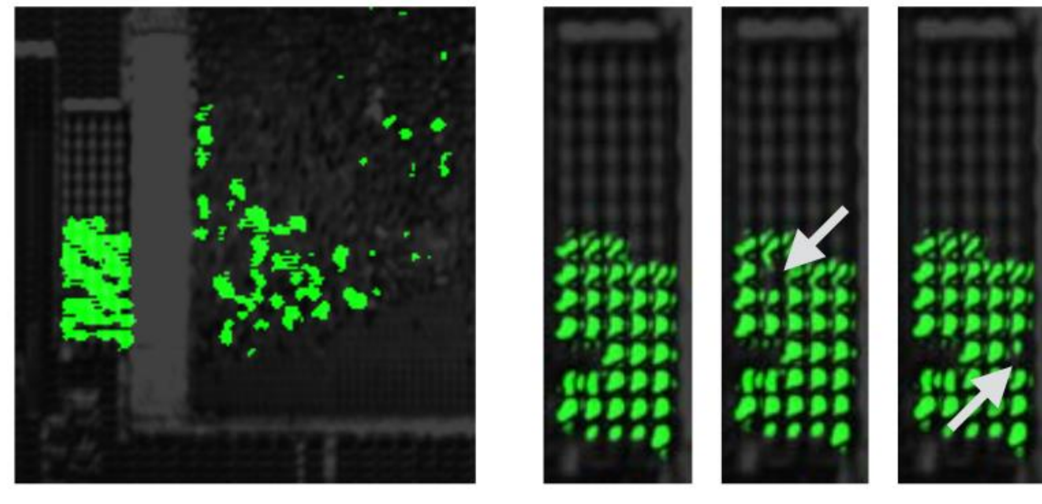
Nabeel et al., in preparation, 2019

Protection of Data and Computation (2)

- (2) External, physical access/modification: probing, photon side channel, etc.



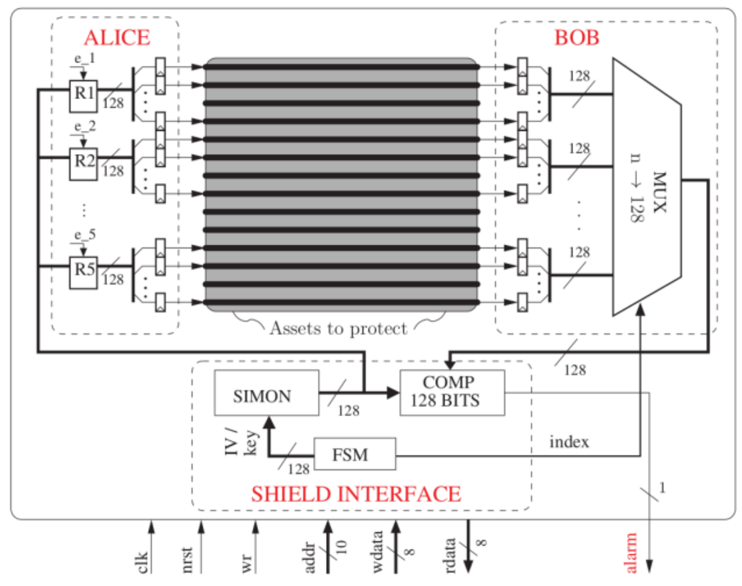
Helfmeier et al., CCS, 2013



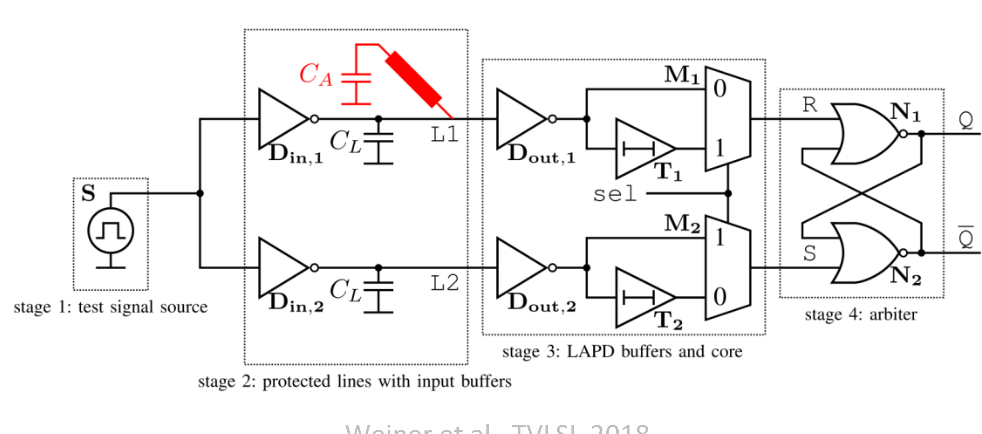
Tajik et al., CCS, 2017

Protection of Data and Computation (2)

- (2) External, physical access/modification: probing, photon side channel, etc.
- Shielding and probing sensors



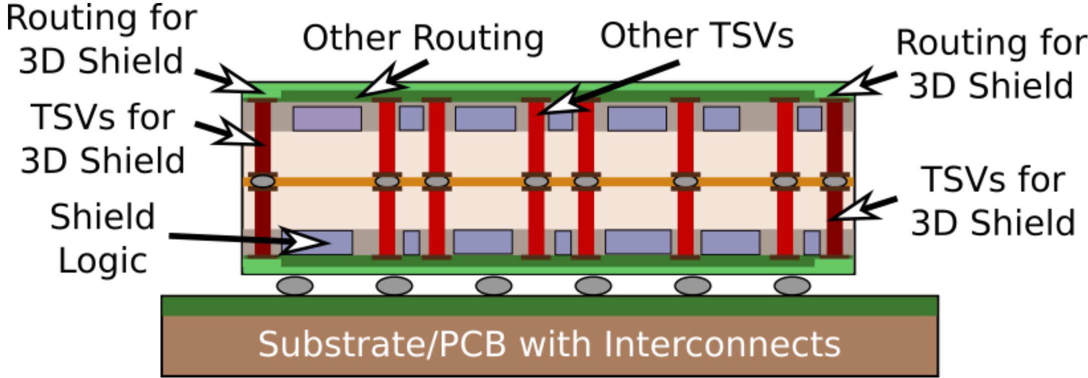
Ngo et al., TC, 2017



Weiner et al., TVLSI, 2018

Protection of Data and Computation (2) **in 3D**

- (2) External, physical access/modification: probing, photon side channel, etc.
- Shielding and probing sensors – <u>“cage all around”</u>
  - Could also block side-channel emissions like photons

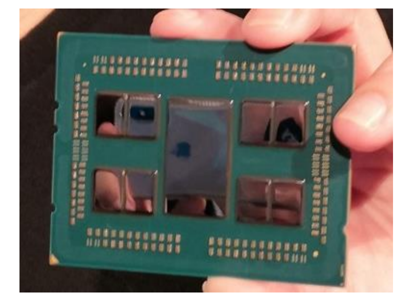


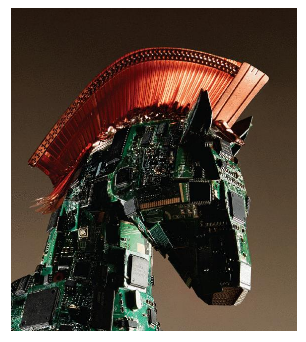
Benefit of 3D Integration: Physical Enclosure

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

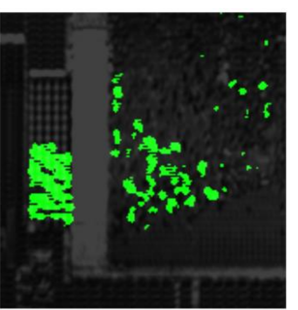
3D Integration: Another Dimension Toward Hardware Security

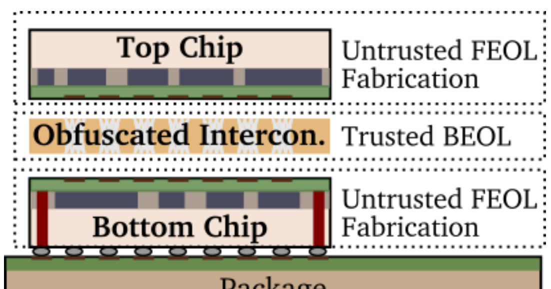
- Data, computation, and hardware itself are at risk
  - Outsourced supply chain: IP piracy, Trojans; design bugs; etc.
  - Attacks at runtime, not only software, also physical ones
- 3D integration: up and coming, "More Moore" and "More than Moore"
- **Physical separation, physical enclosure in 3D for security**

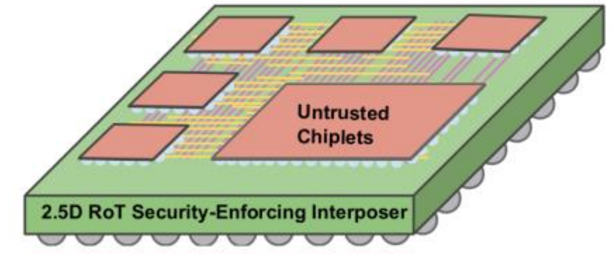


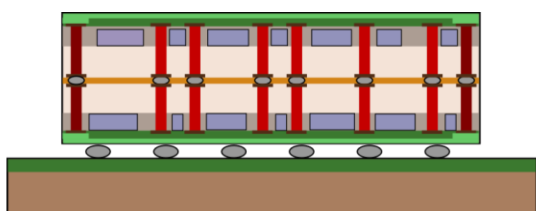


Thank you! johann@nyu.edu









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