جامعة نيويورك أبوظبي
NYU | ABU DHABI

CENTER FOR CYBER SECURITY

DFX LAB
DESIGN FOR EXCELLENCE

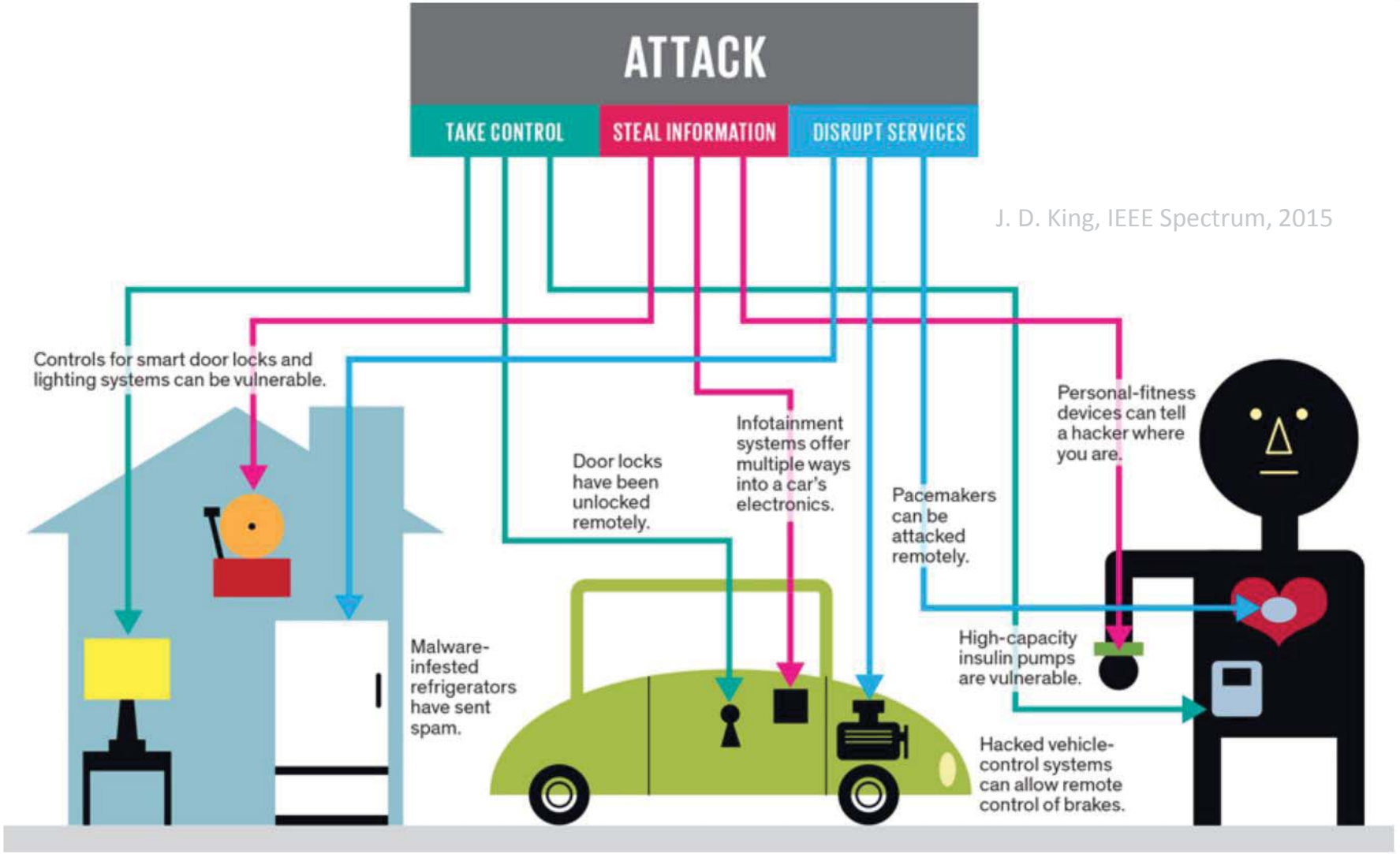
Hardware Security for and beyond CMOS Technology

Johann Knechtel

johann@nyu.edu

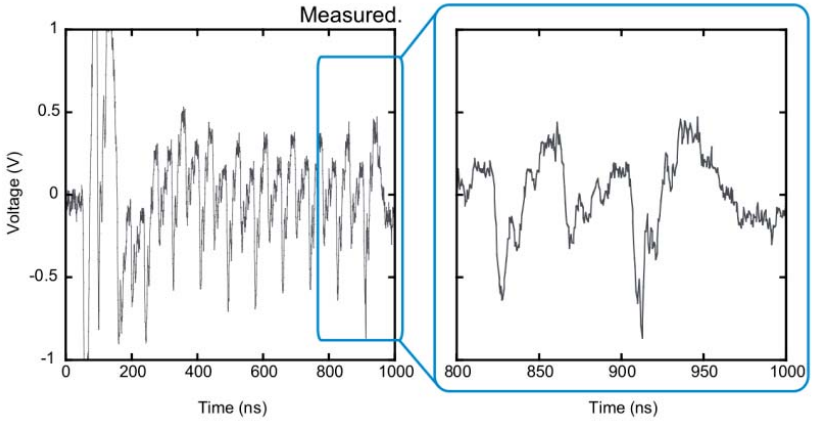
wp.nyu.edu/johann

International Symposium on Physical Design – Online, March 24, 2021

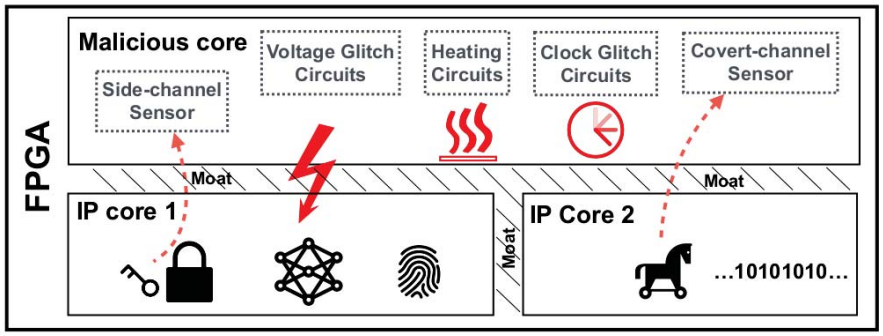


J. D. King, IEEE Spectrum, 2015

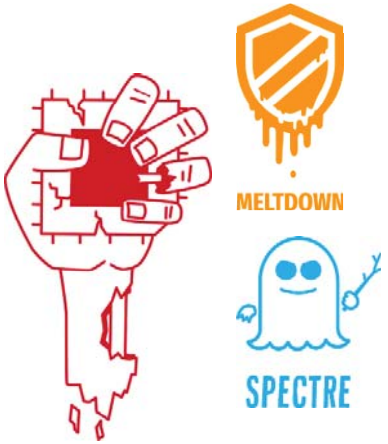
Data and Computation at Risk – Right at the Hardware

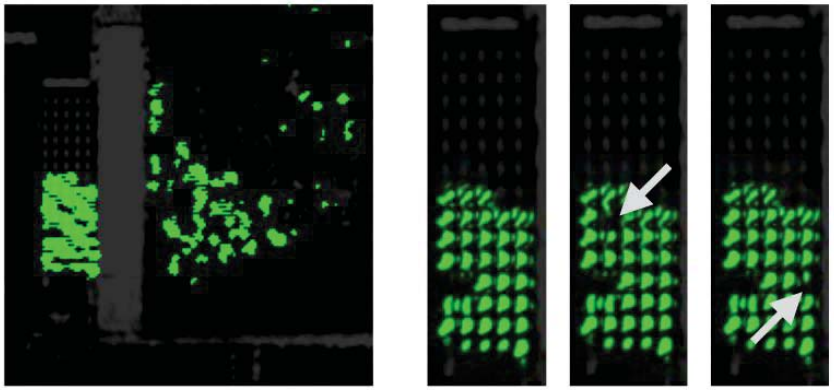


Fujimoto et al., EMC 2014



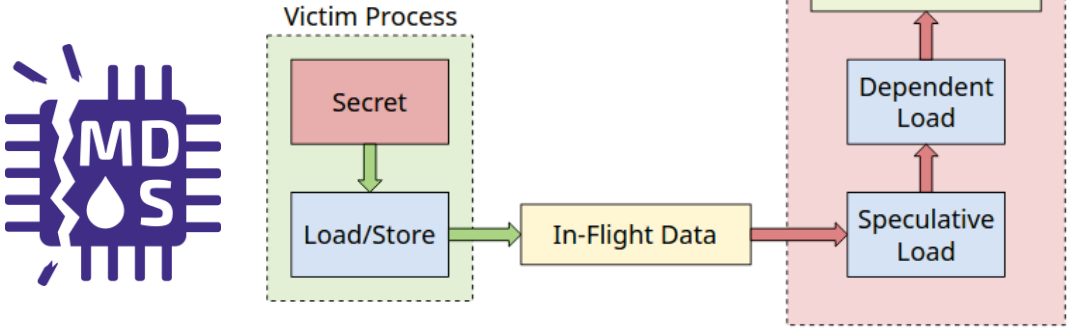
Alam et al., FDTC 2019



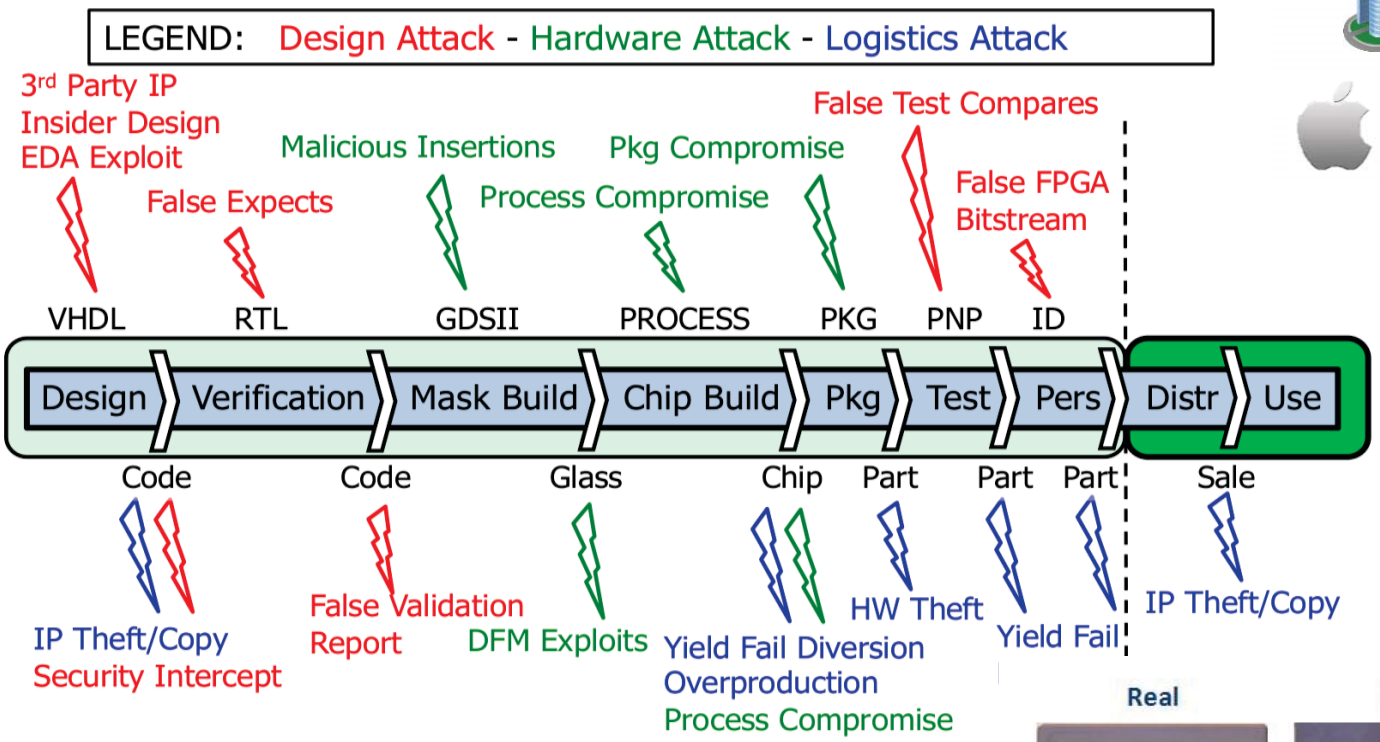


Tajik et al., CCS, 2017

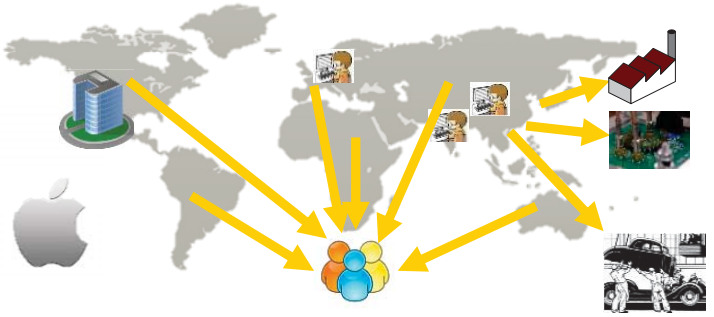
https://www.bleepingcomputer.com, 2019



Hardware Itself Also at Risk



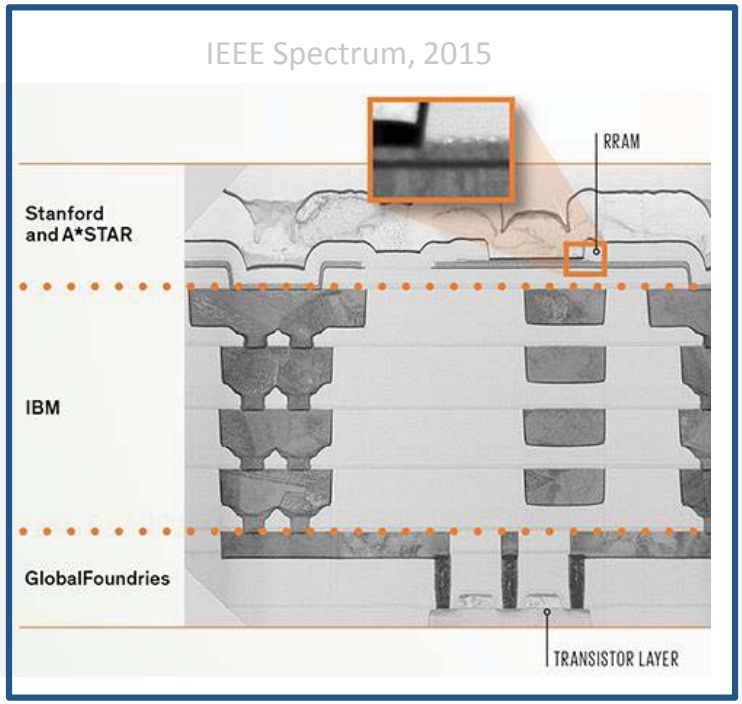
Kerry Bernstein, DARPA, 2016

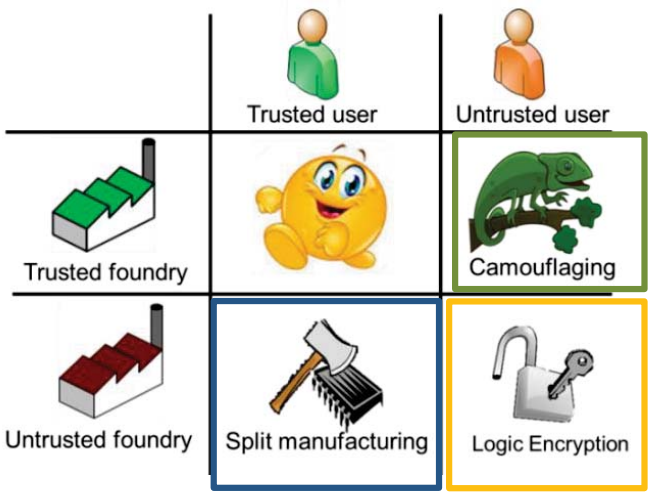


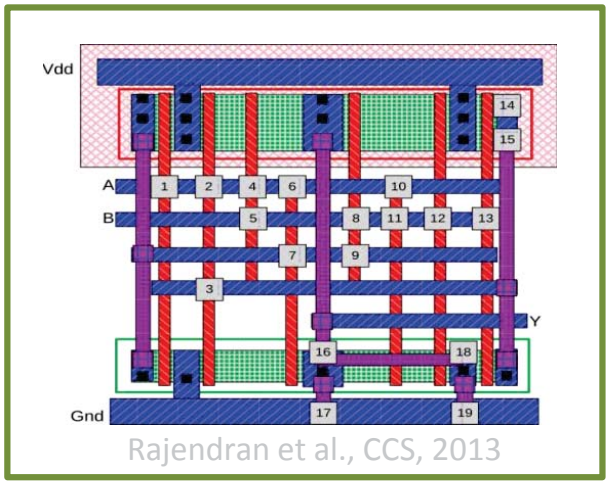
IEEE Spectrum, 2015

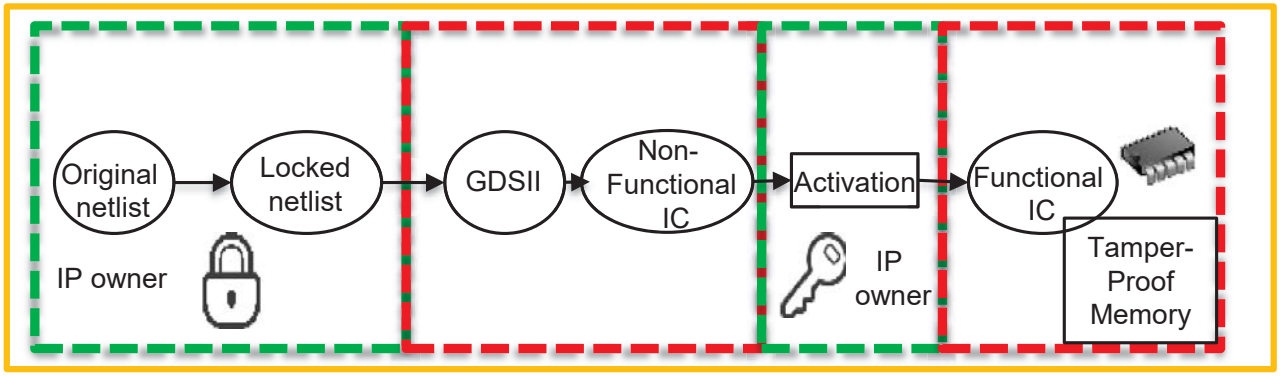
Countermeasures against Attacks on Hardware Itself

- **IP protection**: logic encryption/locking, camouflaging, split manufacturing



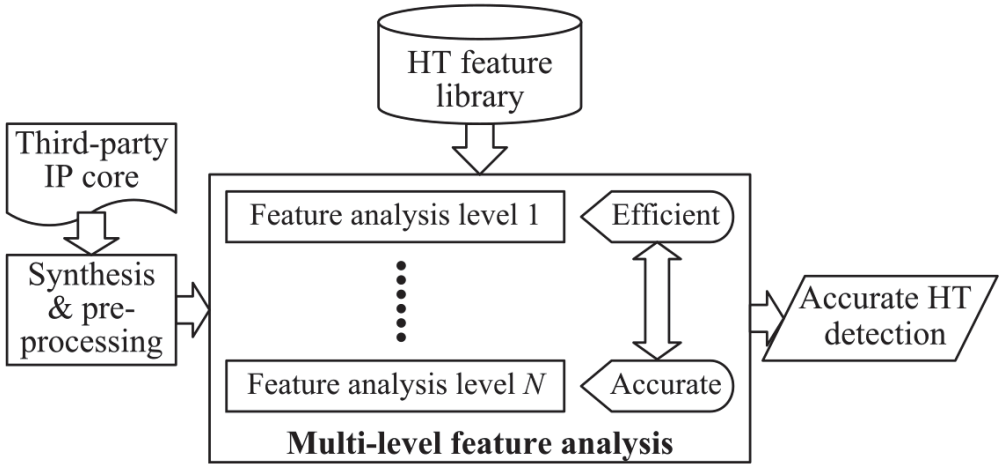




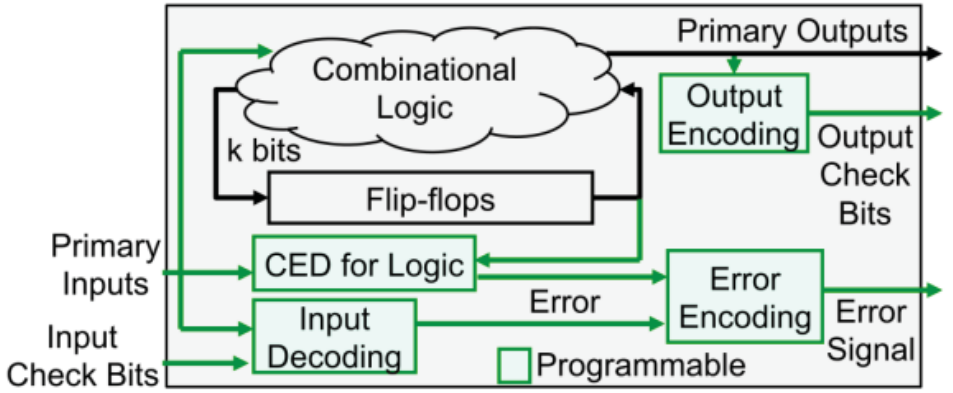


Countermeasures against Attacks on Hardware Itself

- **IP protection**: logic encryption/locking, camouflaging, split manufacturing
- **Trojan defense**: detection, mitigation



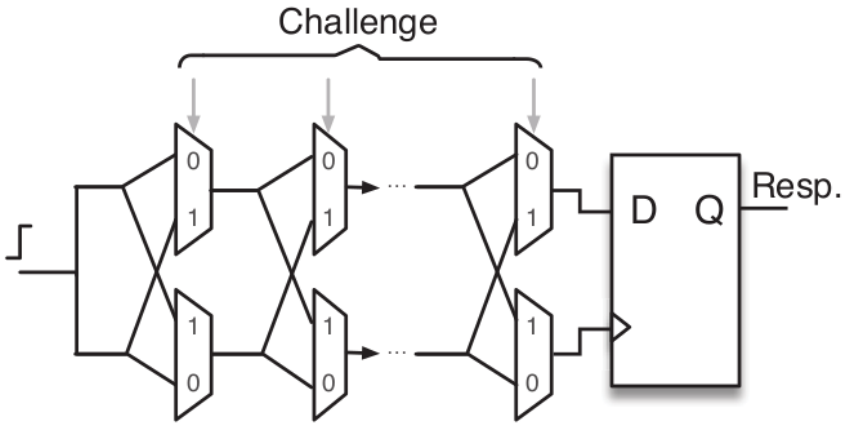
Chen et al., TCAD 2018



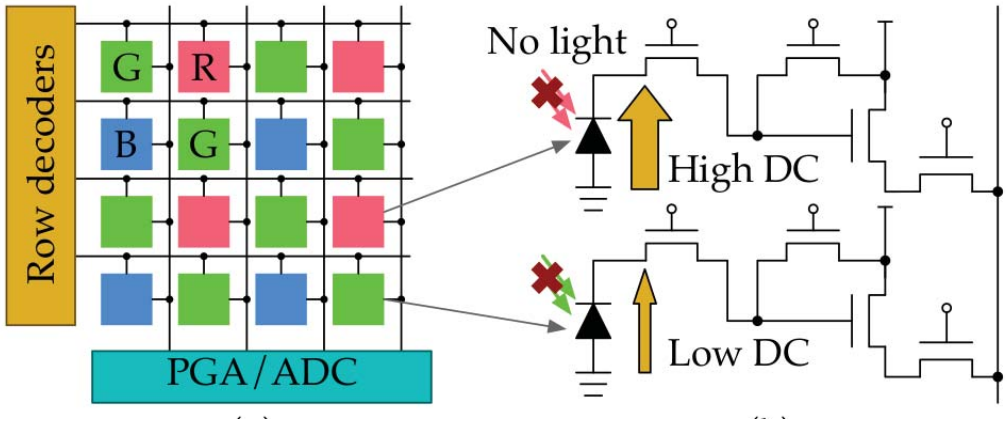
Wu et al., TCAD 2016

Countermeasures against Attacks on Hardware Itself

- **IP protection**: logic encryption/locking, camouflaging, split manufacturing
- **Trojan defense**: detection, mitigation
- **Physically-unclonable functions (PUFs)**: fingerprinting, challenge-response authentication



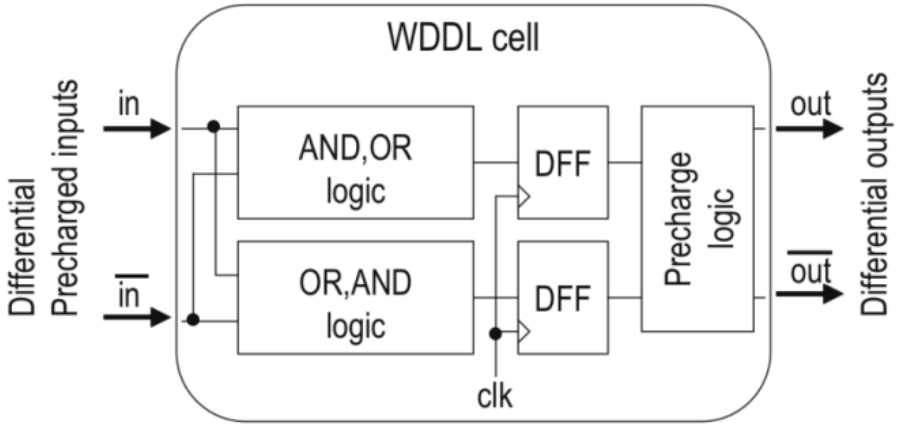
Vatajelu19, IOLTS, 2019



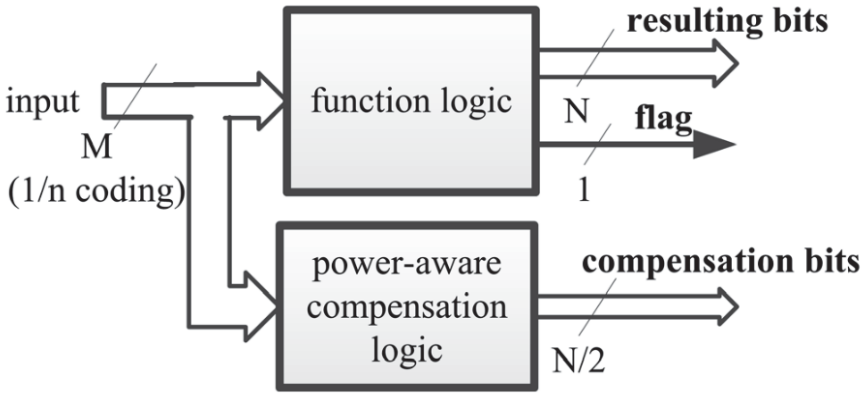
Kim and Lee, DAC, 2018

Countermeasures against Attacks on Data and Computation

- **Masking** against side-channel and fault-injection attacks



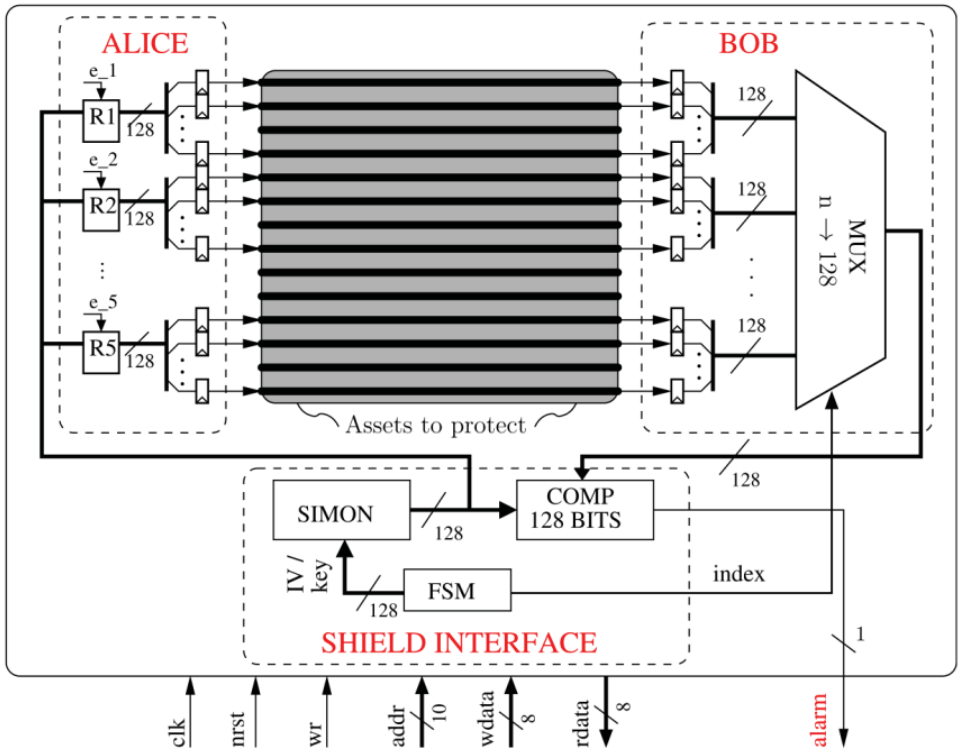
Fujimoto et al., EMC 2014



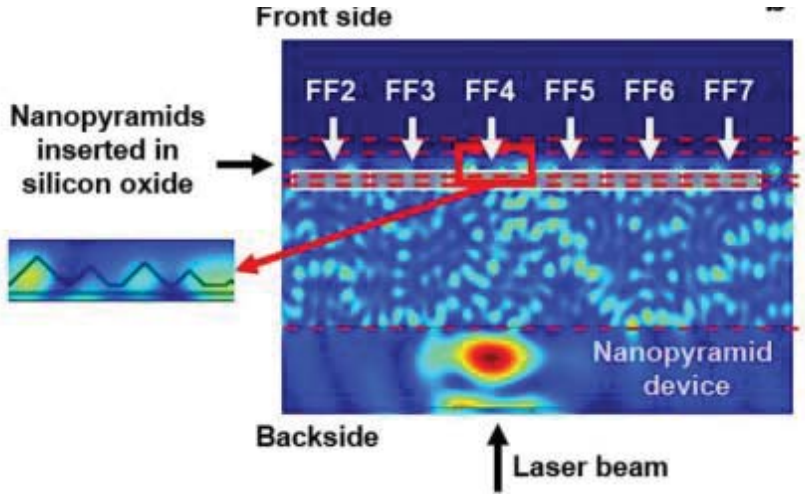
Li et al., TVLSI 2017

Countermeasures against Attacks on Data and Computation

- **Masking** against side-channel and fault-injection attacks
- **Shielding** against probing (front side, back side)

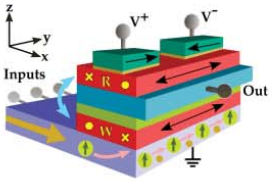


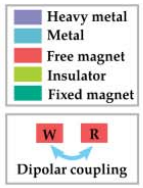
Ngo et al., TC 2017

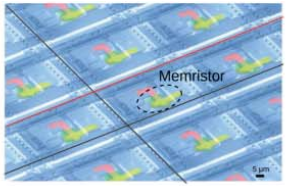


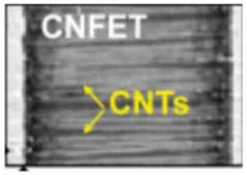
Shen et al., ISTFA 2018

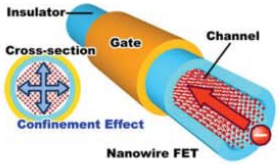
Emerging Technologies for Hardware Security

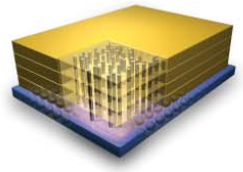


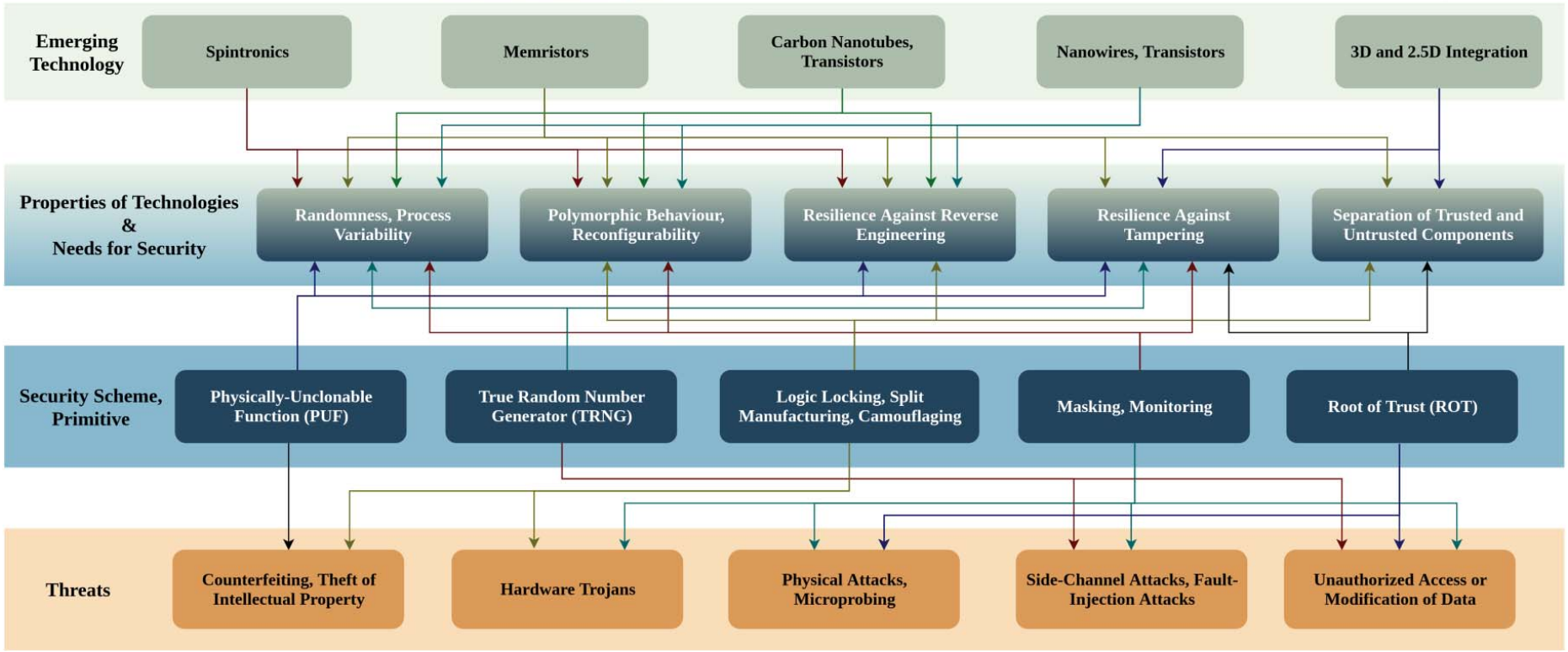




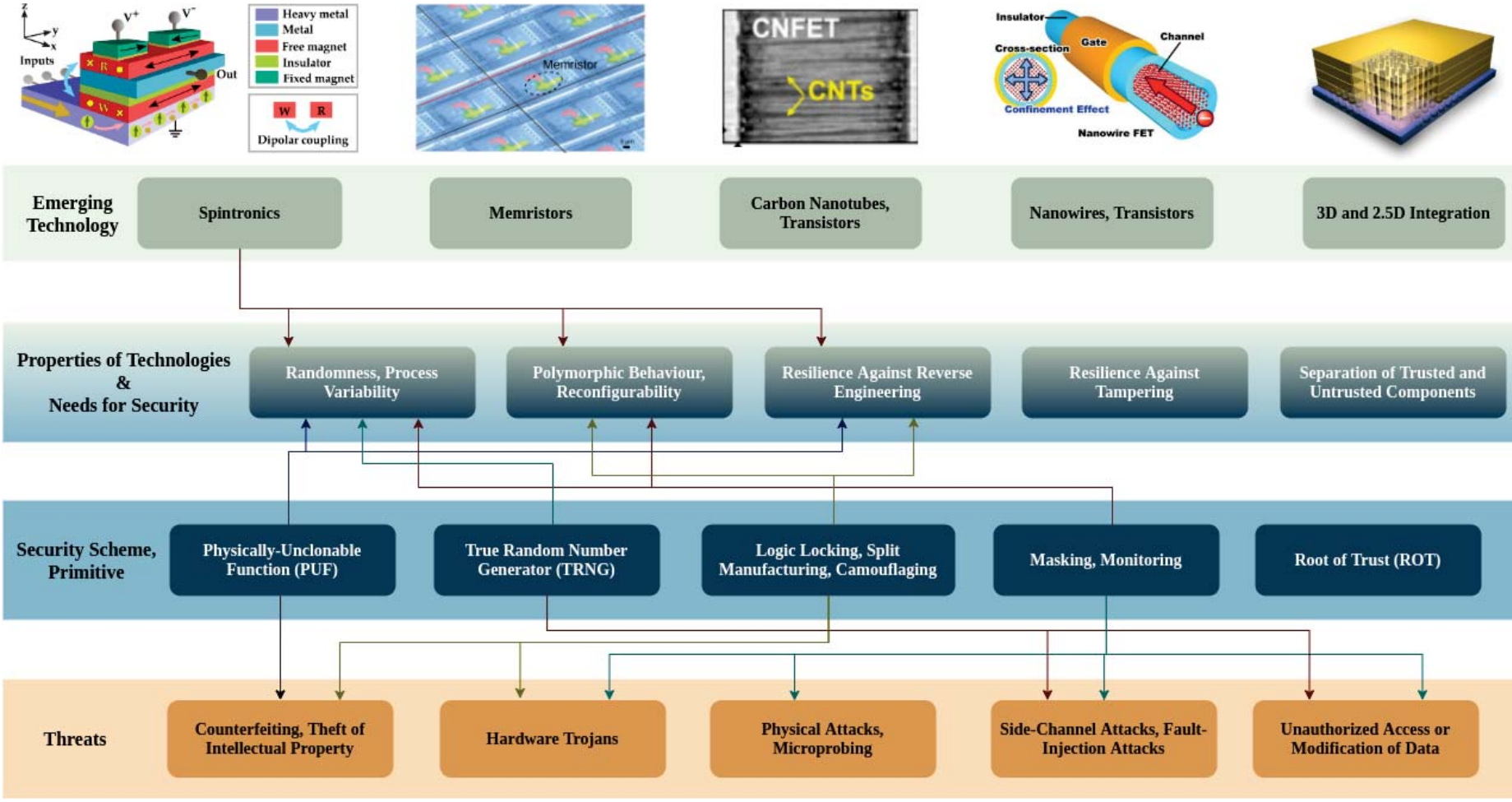






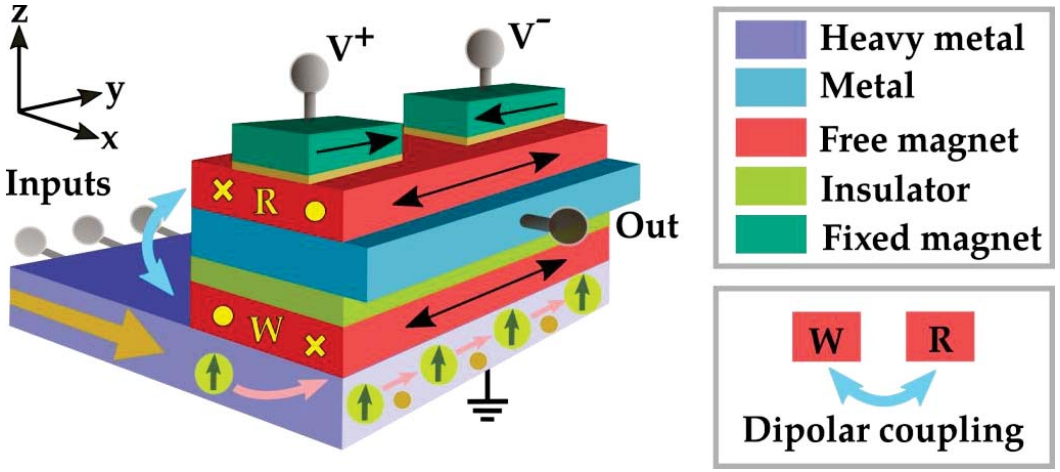


Emerging Technologies for Hardware Security: Spintronics



Basics of Spintronics

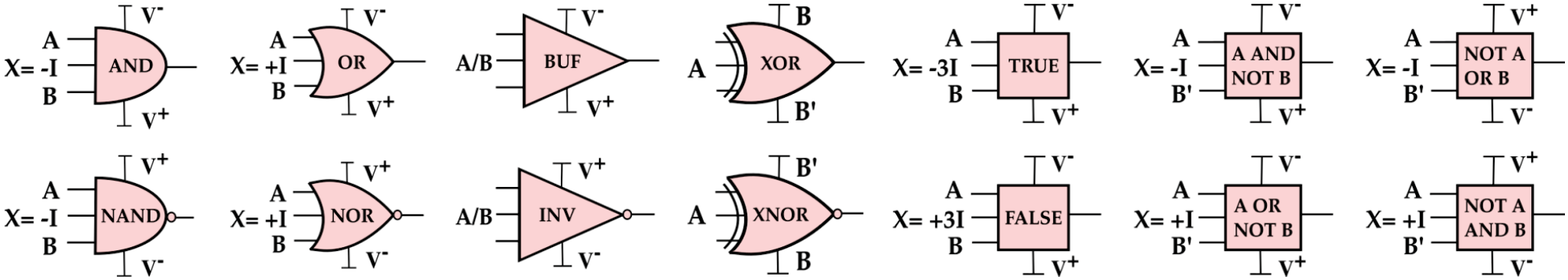
- Besides electronic charge, *spin* of electrons is leveraged for computation and memory
- Switching process is non-volatile, magnetoelectric, and subject to phenomena like spin-transfer torque (STT)
- Typically implemented in BEOL as stack of heavy metals, ferromagnets, and oxide structures; compatible with CMOS



Patnaik et al., TCAD 2019

Basics of Spintronics

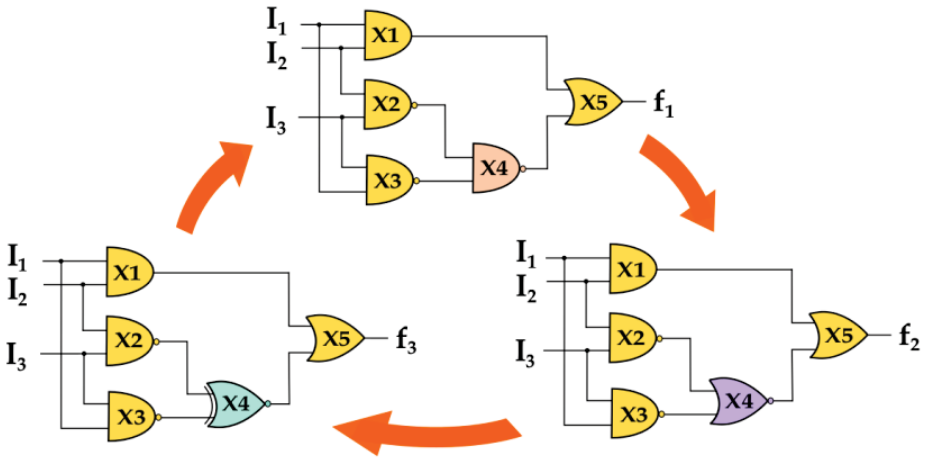
- Compared to CMOS, spintronics can offer lower power consumption, built-in memory functionality, built-in reconfigurability, and better scalability
- Notable efforts by Intel, UC Berkeley, and Berkeley Lab
- Reconfigurable logic, probabilistic computing, and in-memory computing



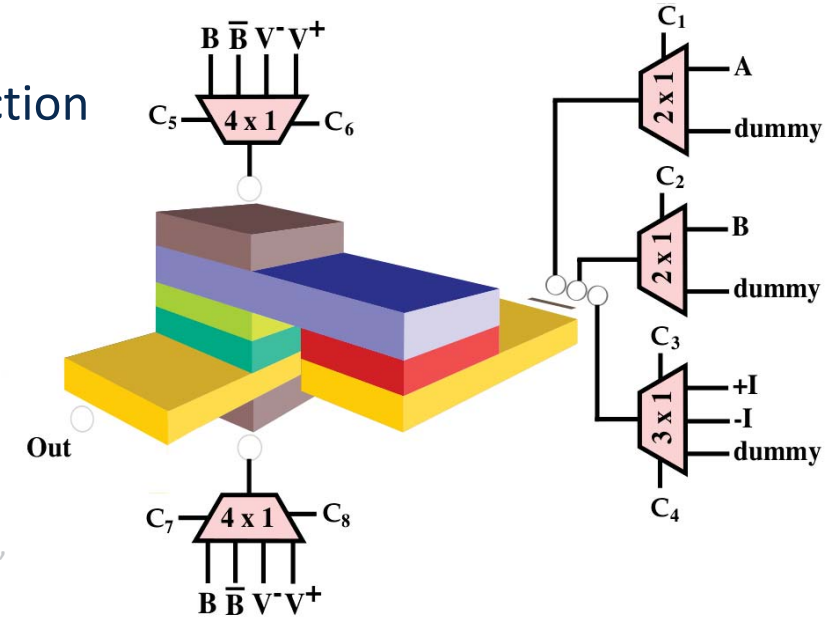
Patnaik et al., TCAD 2019

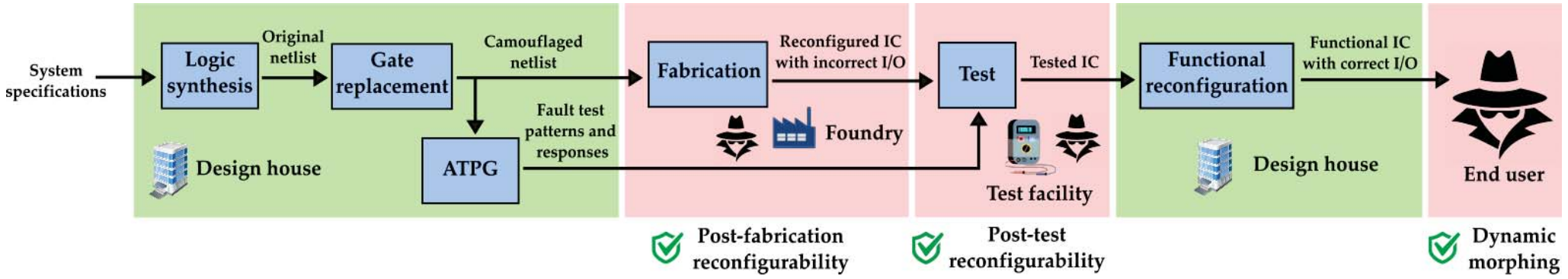
Spintronics for Hardware Security

- **Dynamic camouflaging** as novel paradigm for IP protection



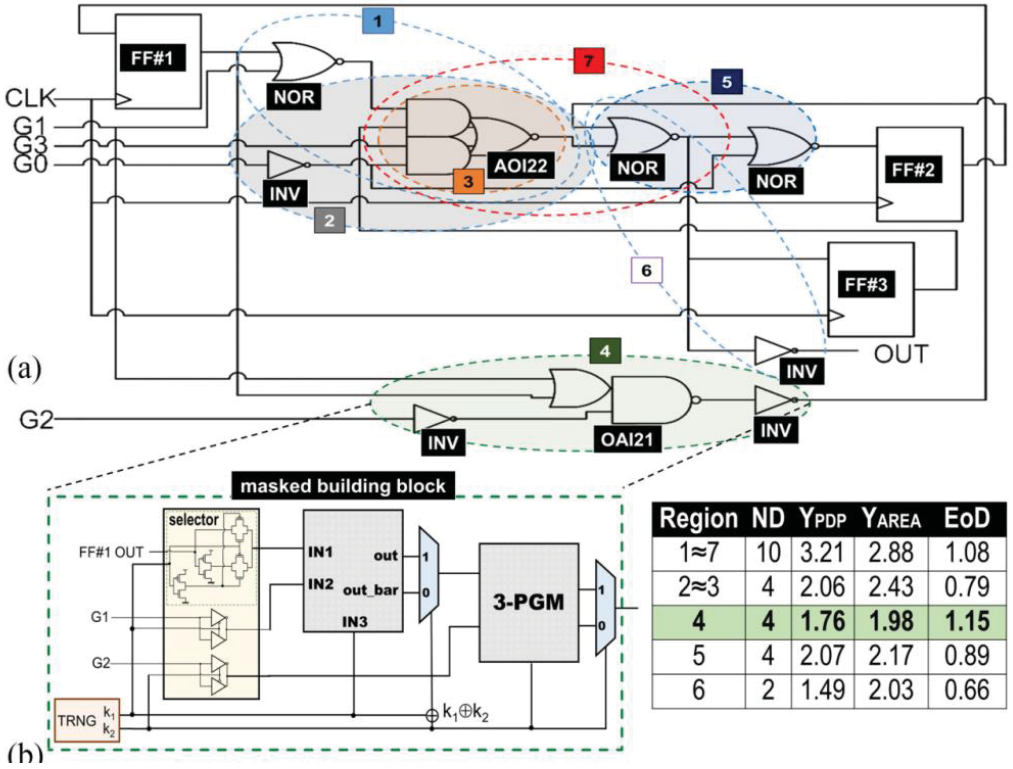
Rangarajan et al., TETC, 2020



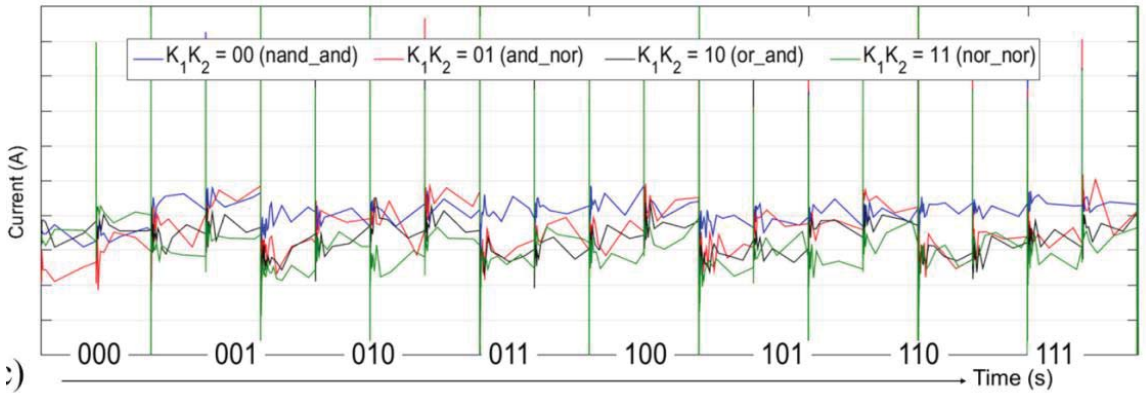


Spintronics for Hardware Security

- **Dynamic camouflaging** as novel paradigm for IP protection
- **Polymorphic, non-CMOS switching** to mitigate side-channel leakage



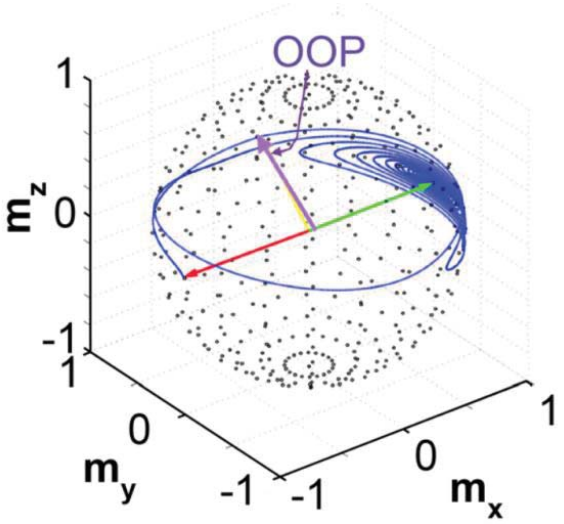
Region	ND	Y_{PDP}	Y_{AREA}	EoD
1≈7	10	3.21	2.88	1.08
2≈3	4	2.06	2.43	0.79
4	**4**	**1.76**	**1.98**	**1.15**
5	4	2.07	2.17	0.89
6	2	1.49	2.03	0.66

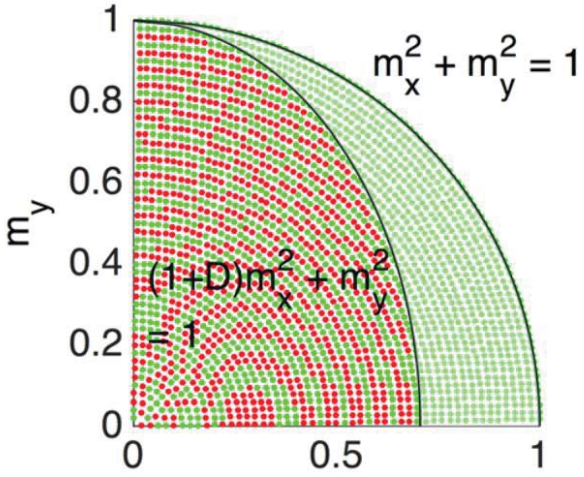


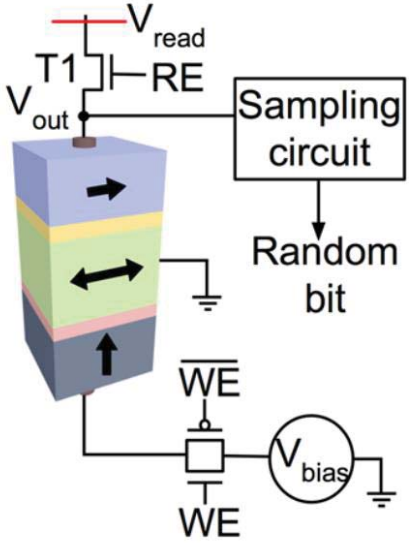
Roohi et al.,
TNANO, 2019

Spintronics for Hardware Security

- **Dynamic camouflaging** as novel paradigm for IP protection
- **Polymorphic, non-CMOS switching** to mitigate side-channel leakage
- **Tunable switching processes** for PUFs and TRNGs

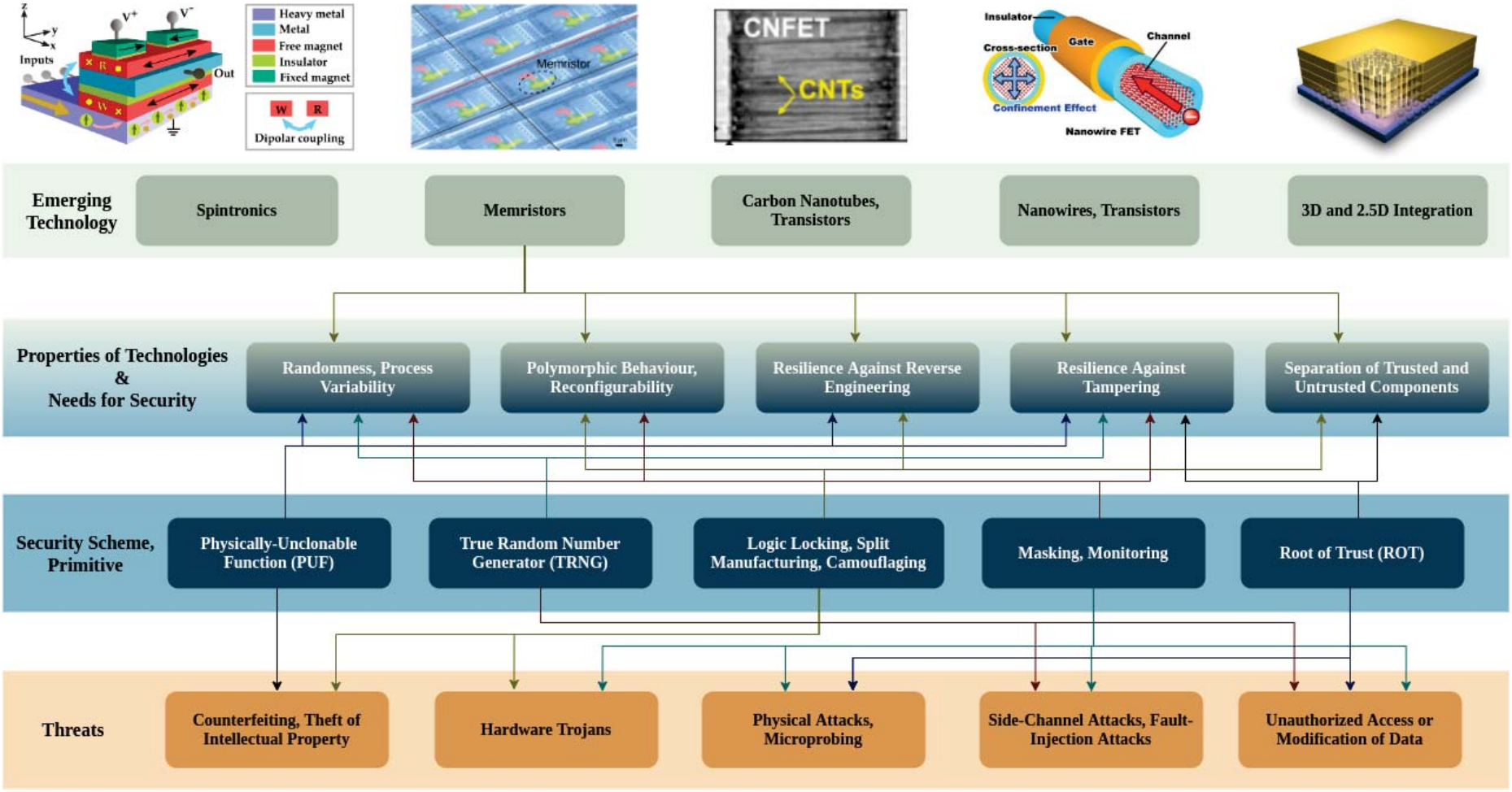






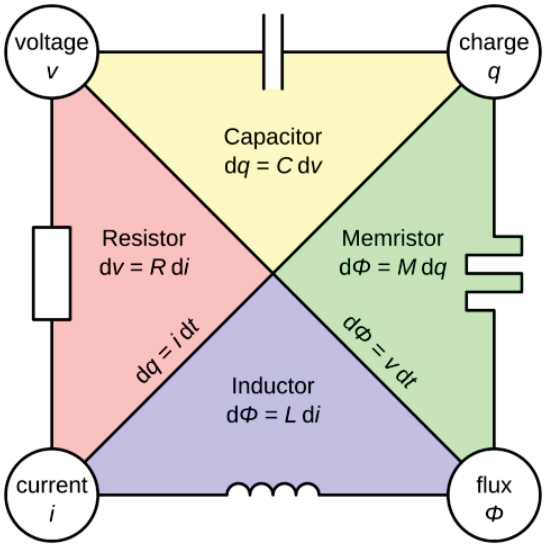
Rangarajan et al., JAP, 2017

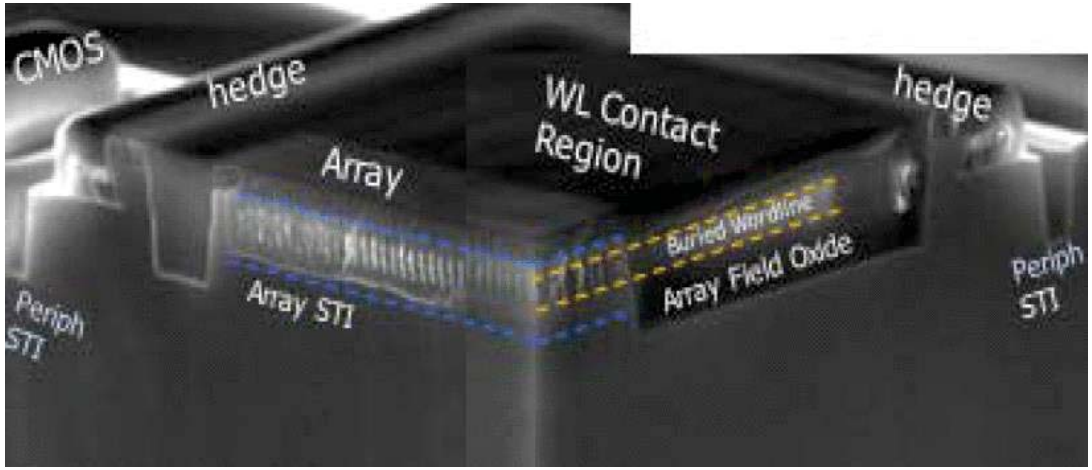
Memristors for Hardware Security



Basics of Memristors

- Memory resistor, another fundamental circuit element
- Retain an internal resistive state according to the history of voltage or current applied
- For some, nonlinear response (pinched hysteresis loops)
- R&D considering various materials and arrangements like titanium dioxide – can be made compatible with CMOS

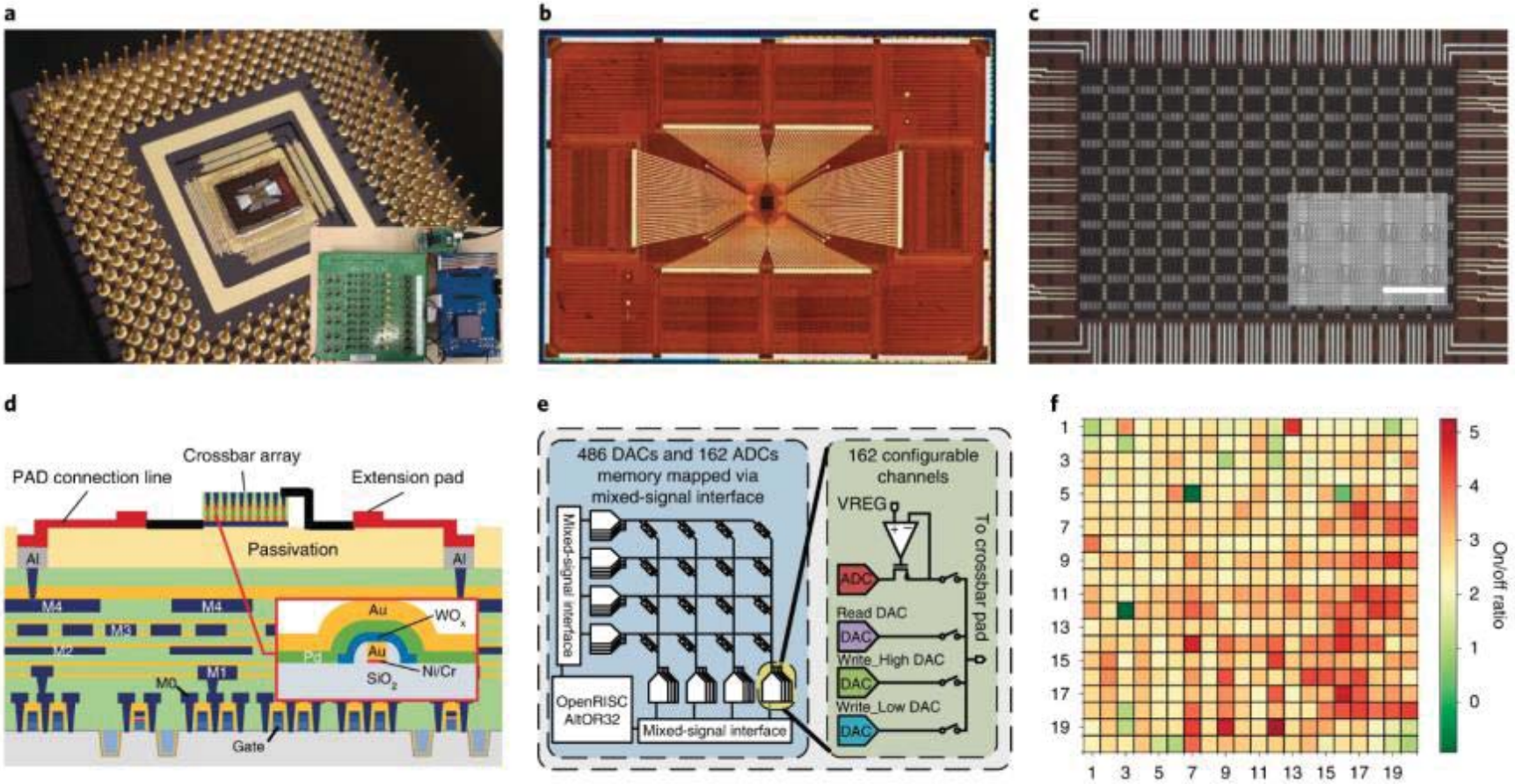




Zahurak et al., IEDM 2014

Basics of Memristors

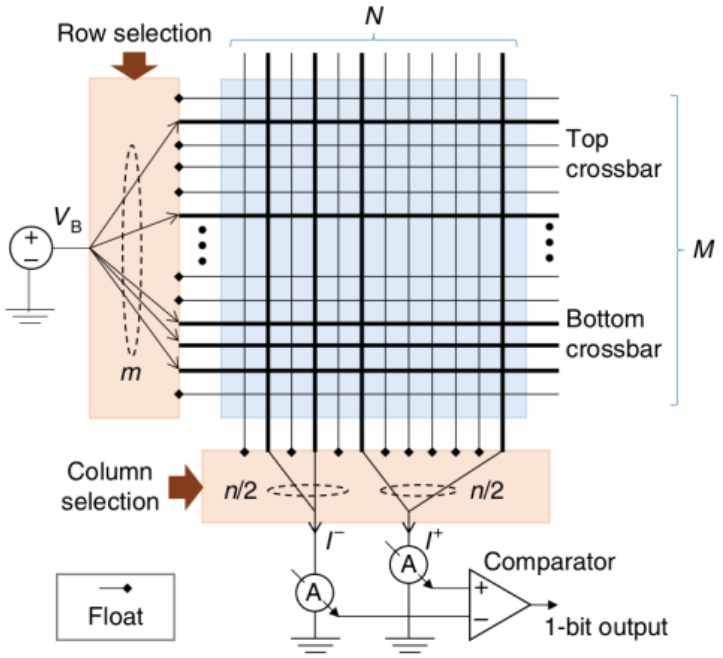
- In-memory computing, neuromorphic computing, and reconfigurable logic



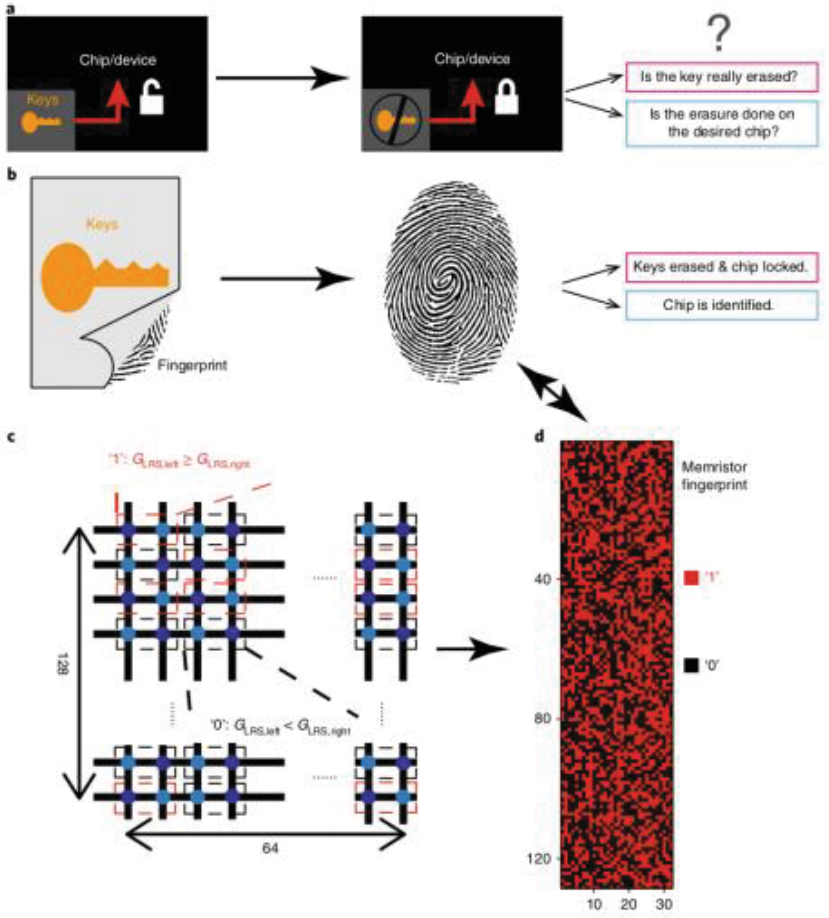
Cai et al., Nature 2019

Memristors for Hardware Security

- Nonlinear variations for PUFs
- Secure key management, e.g., for locking
- IP protection via by polymorphic behavior and separation of components

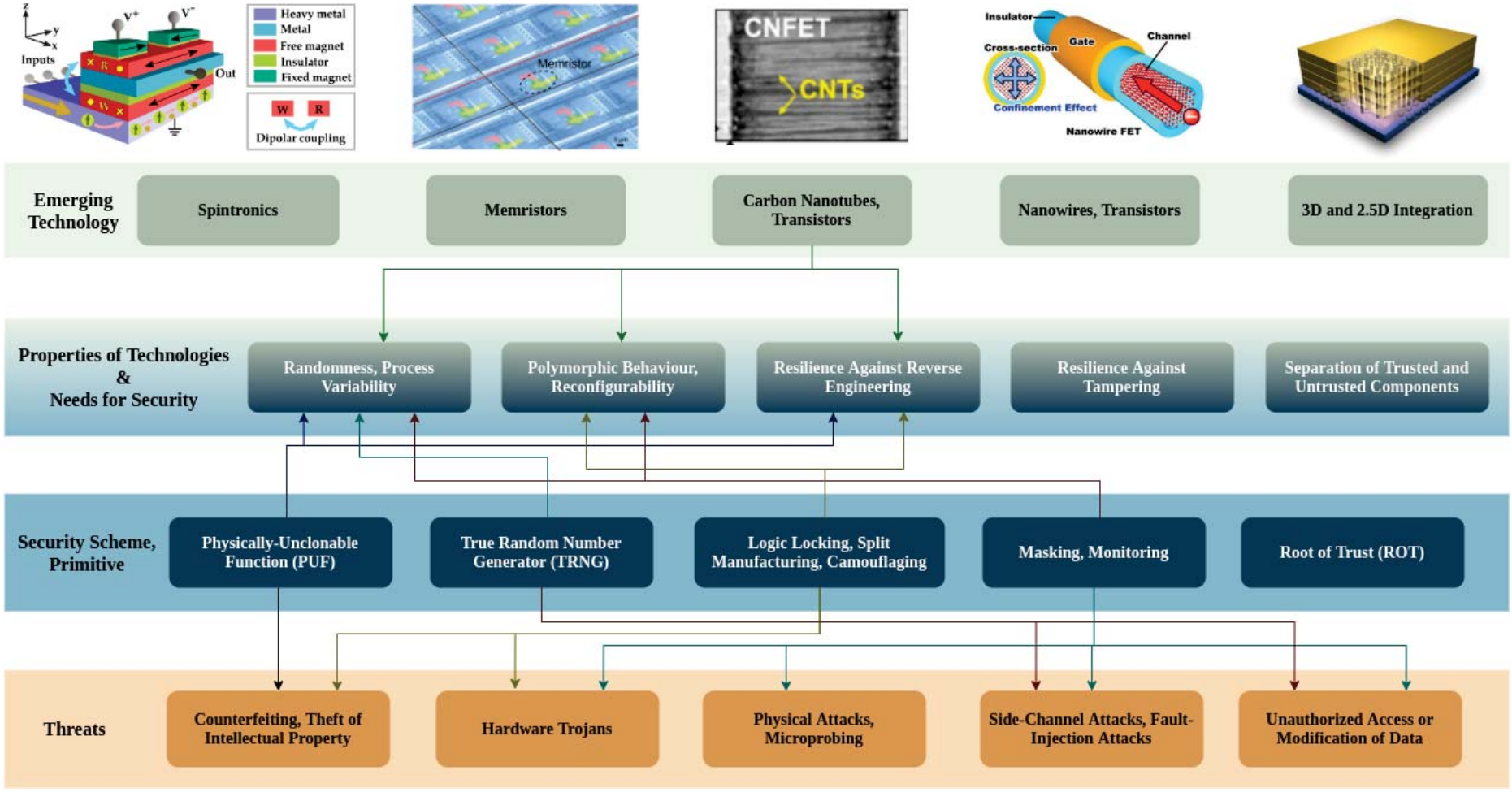


Nili et al., Nature 2018



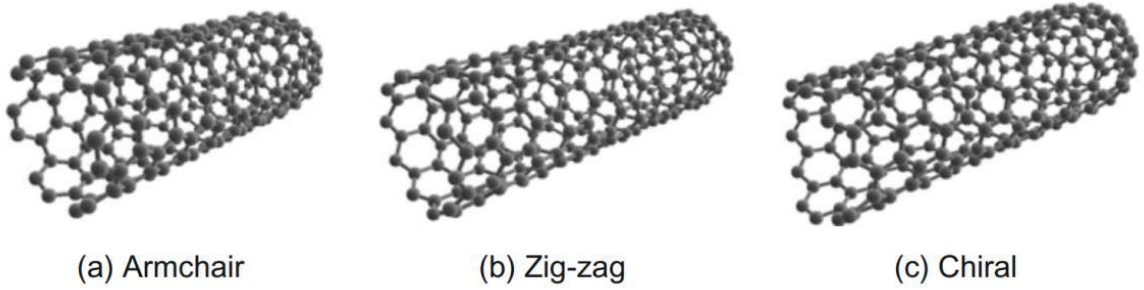
Jiang et al., Nature 2018

Carbon Nanotubes for Hardware Security

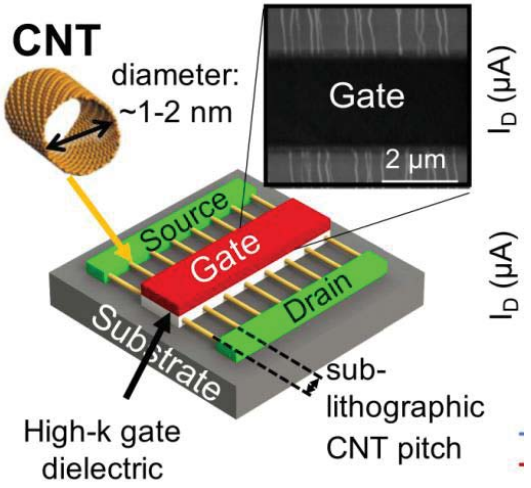


Basics of Carbon Nanotube Transistors

- Carbon nanotubes (CNTs): one or more rolled-up layers of graphene, the planar arrangement of single-layer carbon atoms in 2D honeycomb-like structures
- Either metallic conductors or semiconductors, depending on structure
- Outstanding electrical, physical, and thermal properties
  - Due to the strong bonds between C atoms
  - Individual metallic CNTs can hold current densities more than 1,000 times greater than copper
- Used for interconnects and transistors

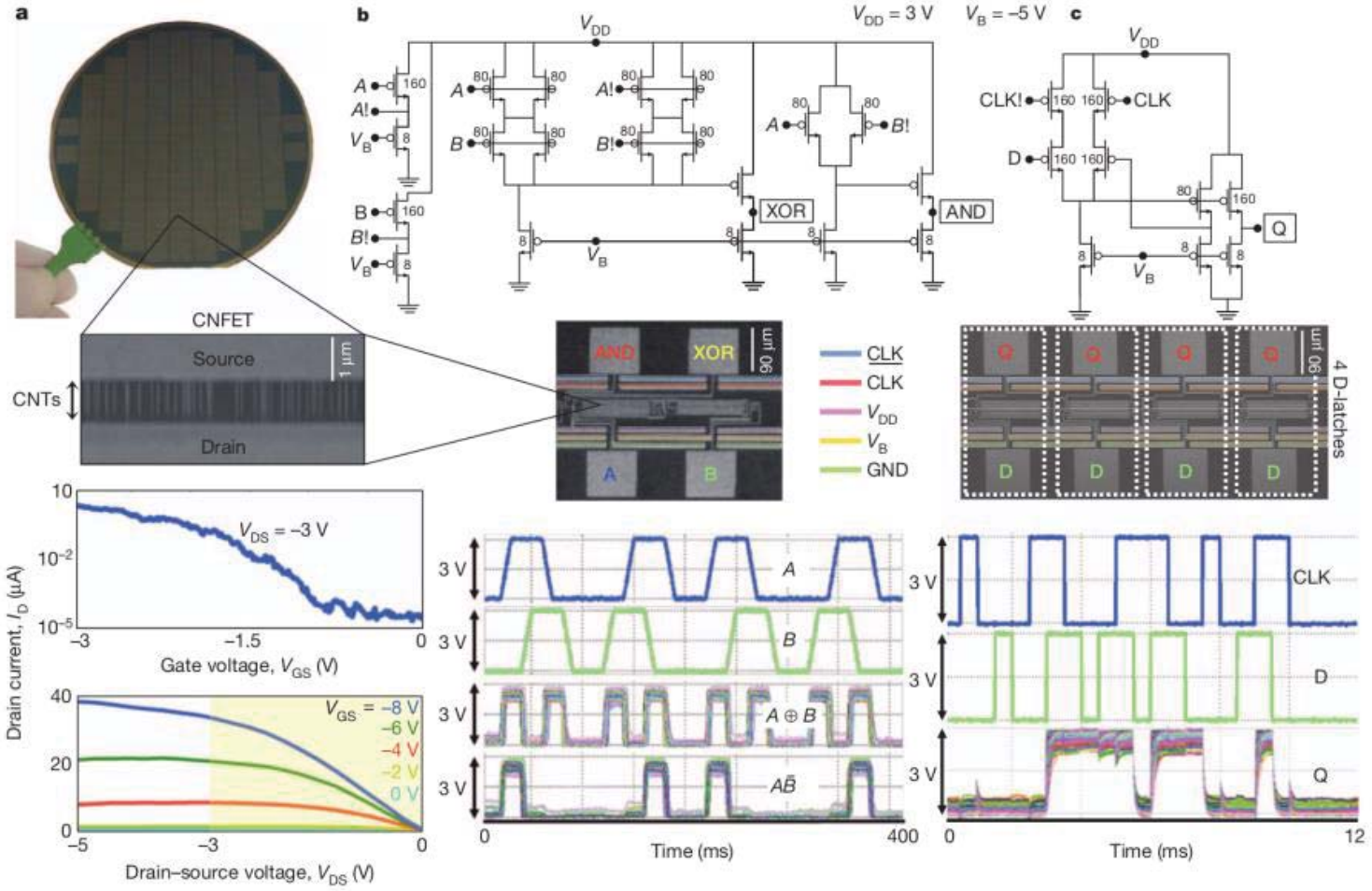


Lienig and Thiele, Springer, 2018



Wu et al., JSSC 2018

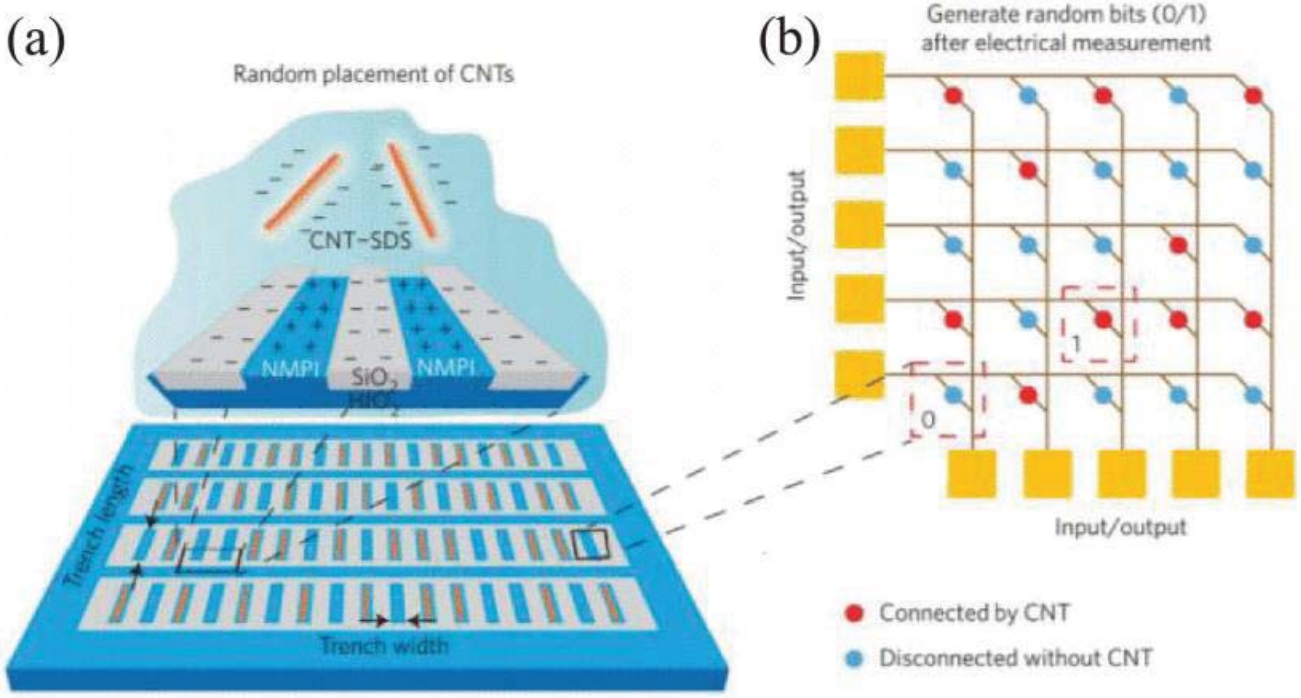
Basics of Carbon Nanotube Transistors



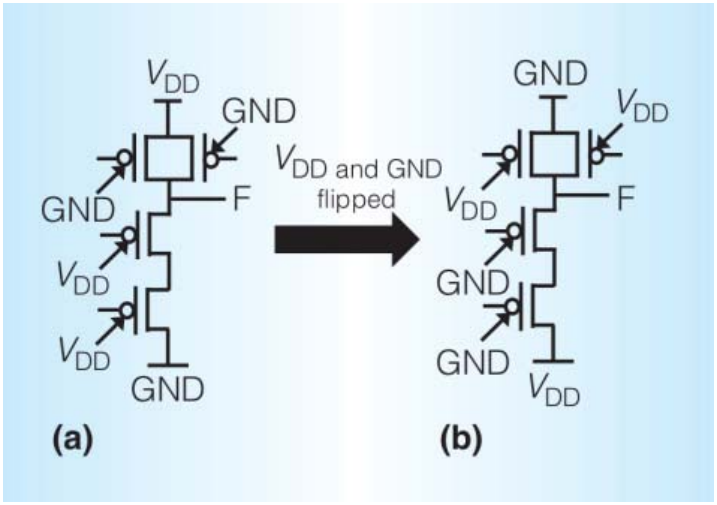
Shulaker et al., Nature 2013

Carbon Nanotubes for Hardware Security

- Manufacturing variability for PUFs and TRNGs
- IP protection by reconfigurablity

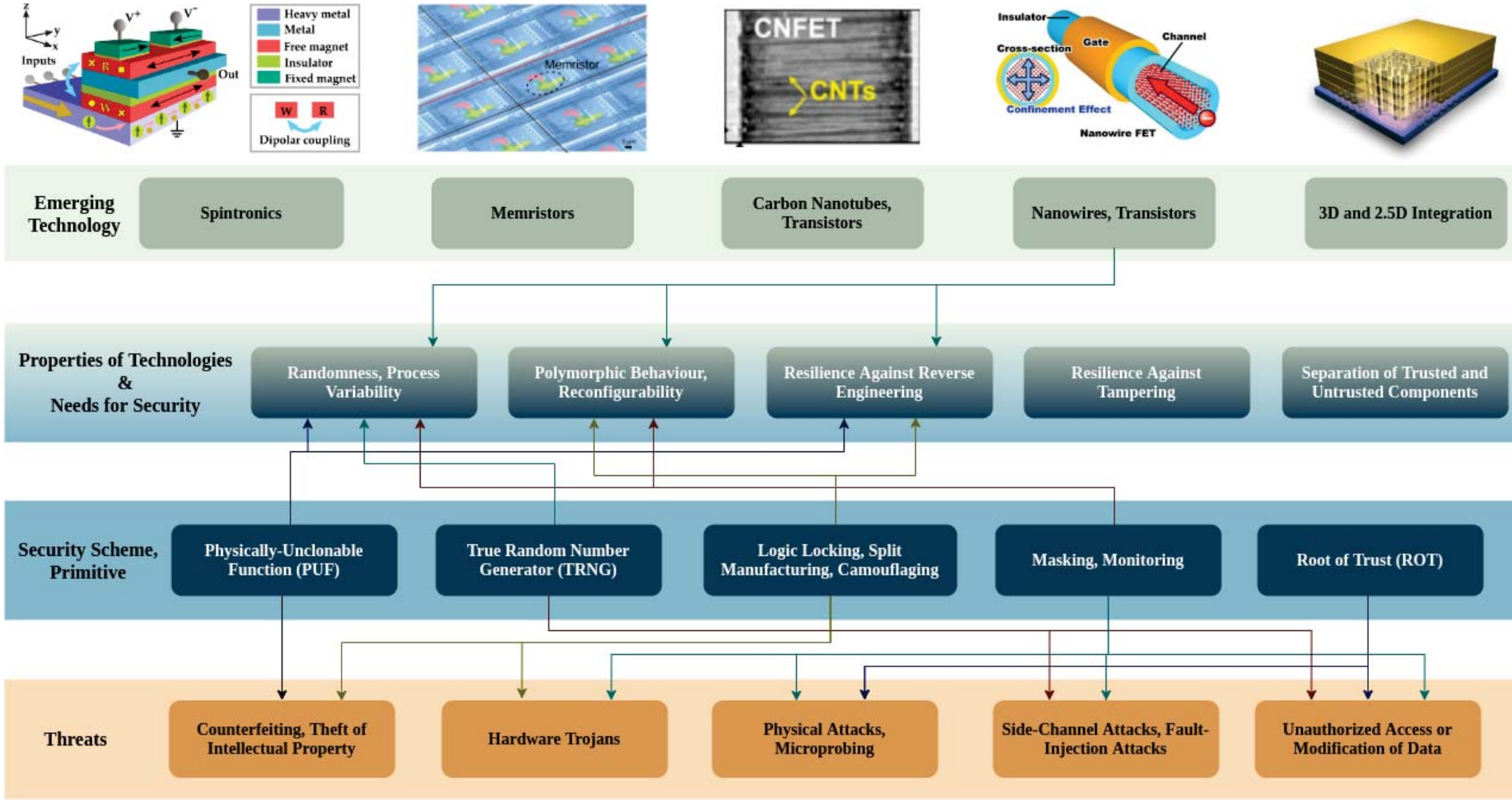


Rahman et al., TVLSI, 2017



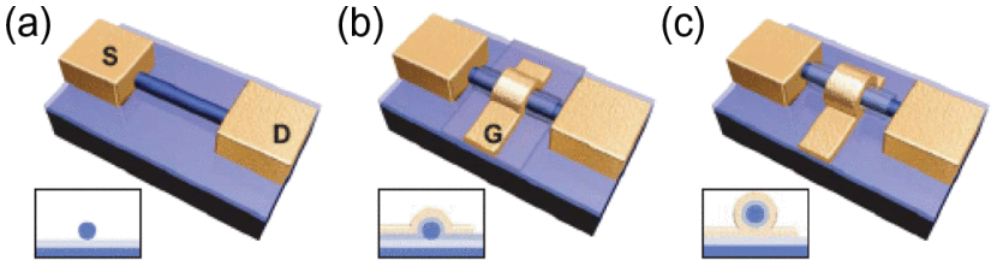
Suresh et al., Micro, 2016

Emerging Technologies for Hardware Security: Nanowire Transistors

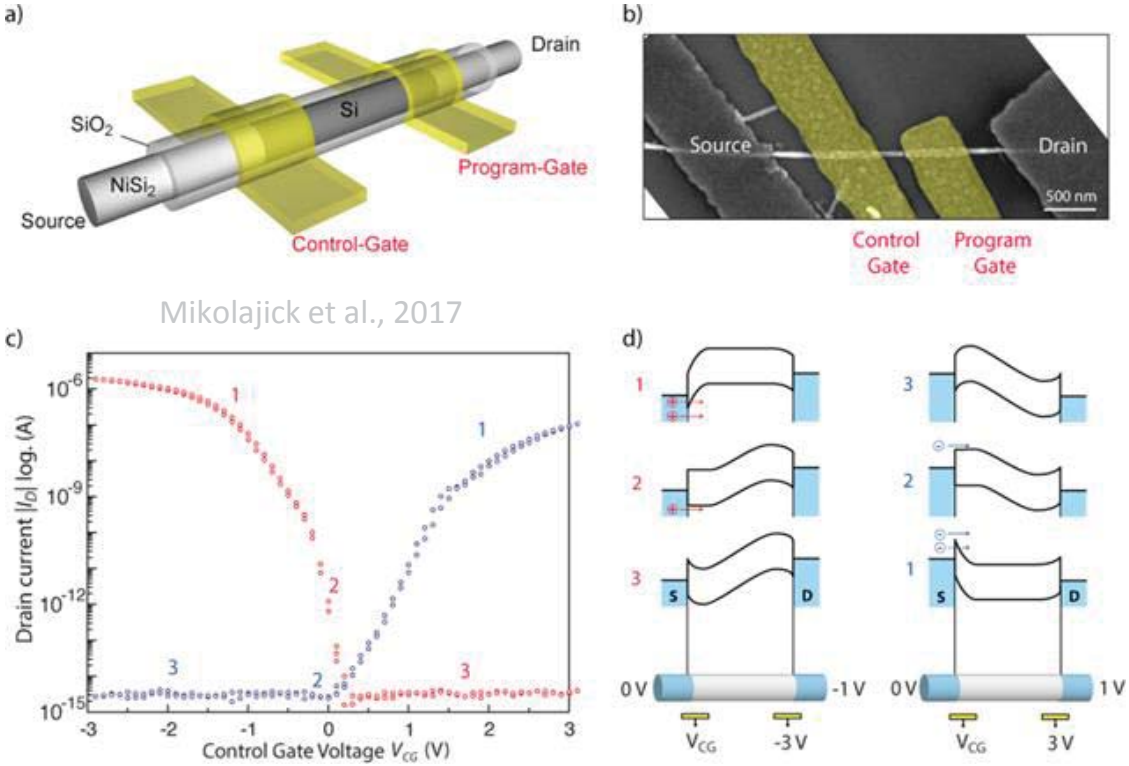


Basics of Nanowire Transistors

- Nano-scaled and semiconductive wires as transistor channel
- Somewhat similar to CNT-FETs, but allow for finer control of desired properties (whereas CNT-FETs offer better performance)
- Sensing applications, flexible electronics, and reconfigurable logic



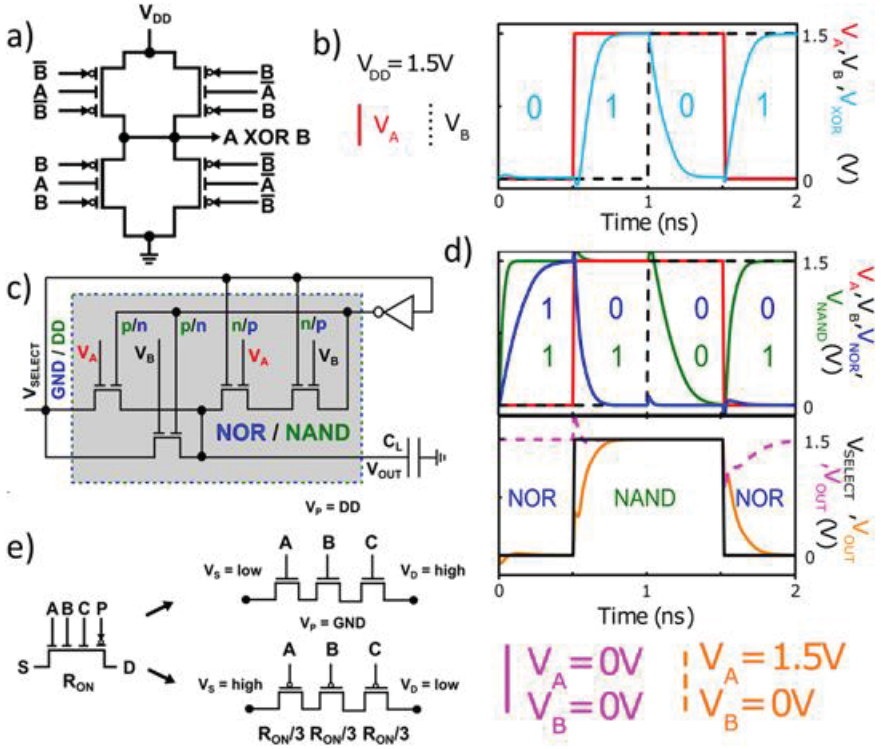
Lu et al., TED 2008



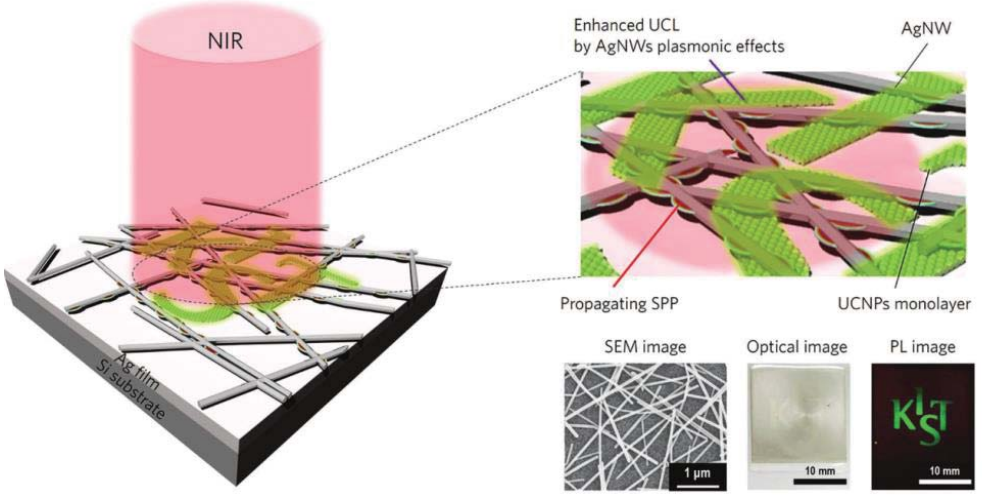
Mikolajick et al., 2017

Nanowire Transistors for Hardware Security

- Controllable ambipolarity and polymorphic behavior for IP protection
- Plasmonic interaction for tagging

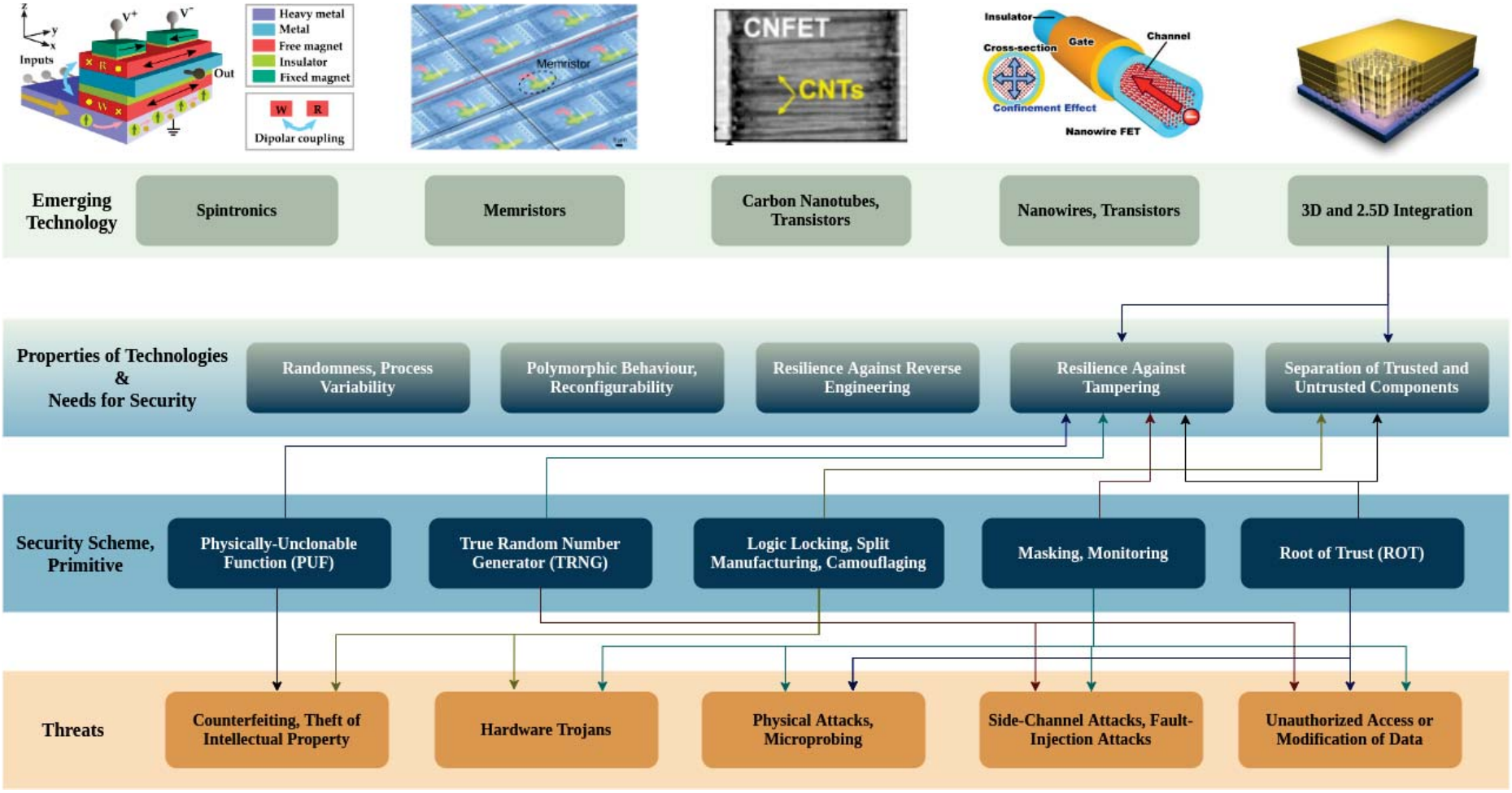


Mikolajick et al., 2017



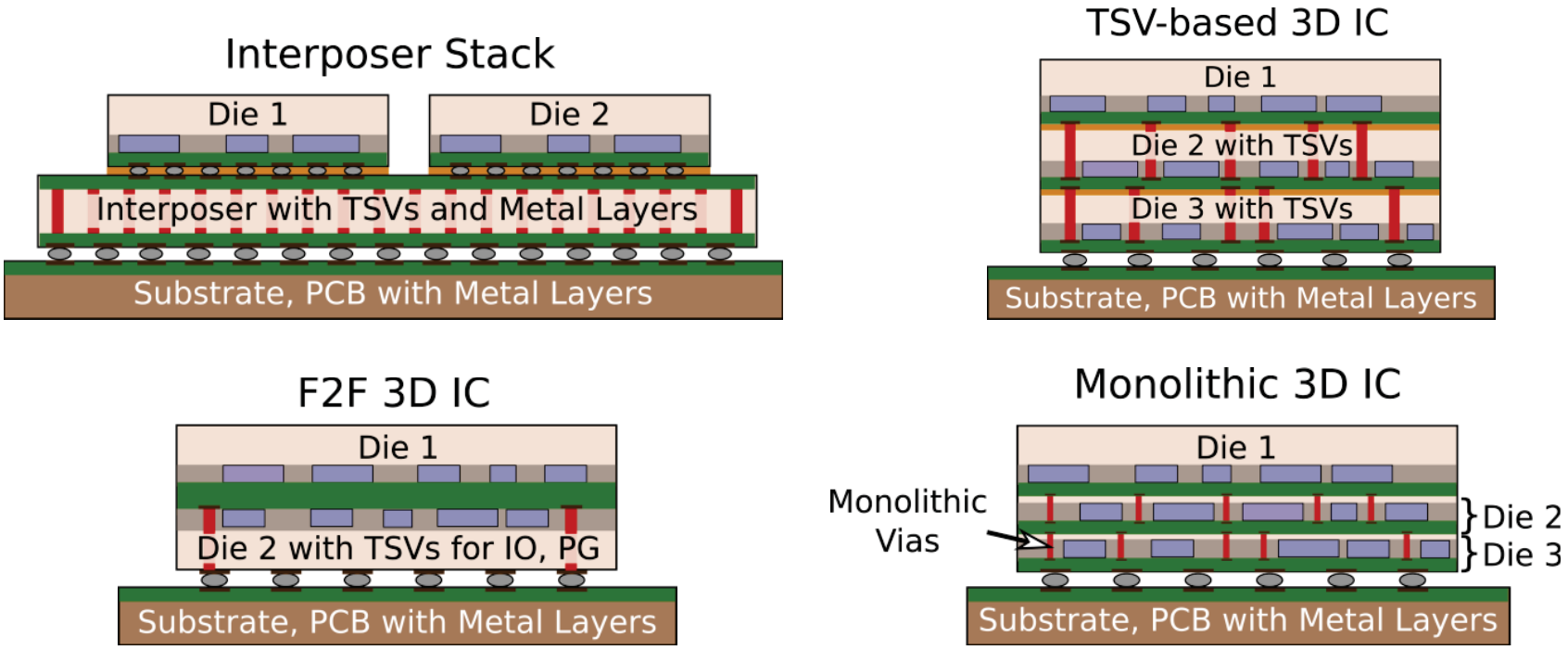
Park et al., 2016

Emerging Technologies for Hardware Security: 2.5D and 3D Integration

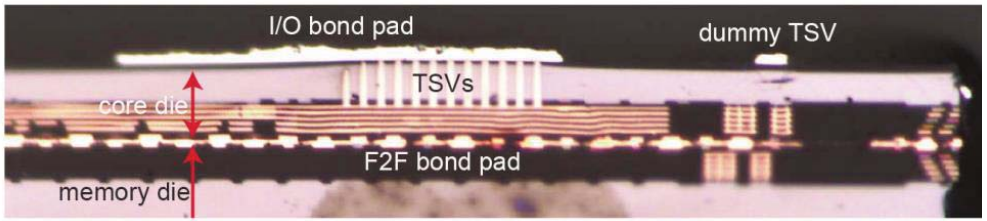


Basics of 2.5D and 3D Integration

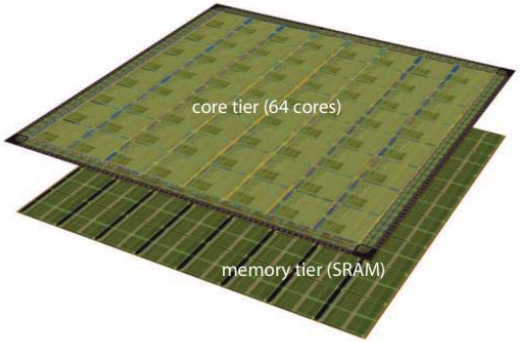
- **Shorter, vertical interconnects:** power consumption, delay, bandwidth – "More Moore"
- **Separate dies integrated:** heterogeneous, large systems; yield – "More than Moore"

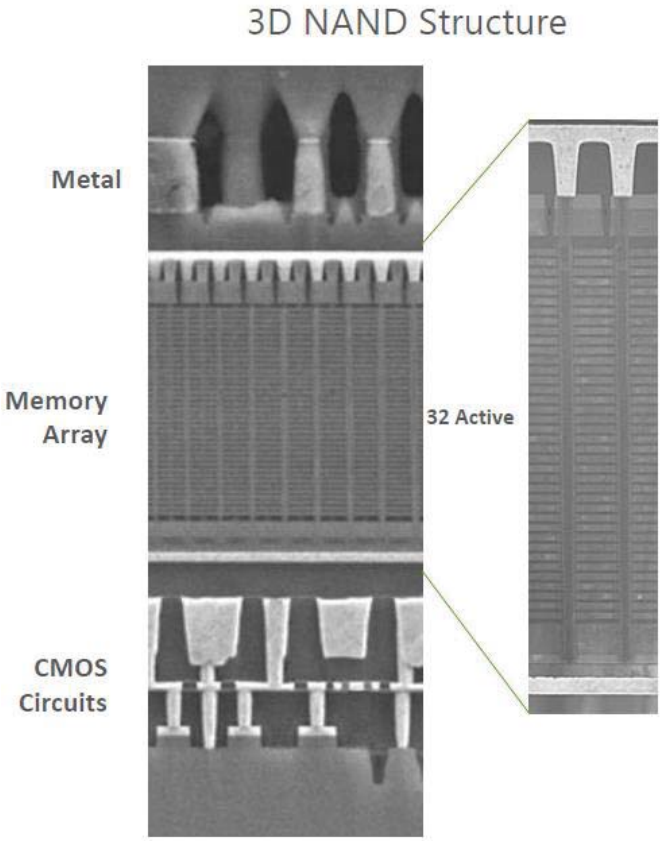


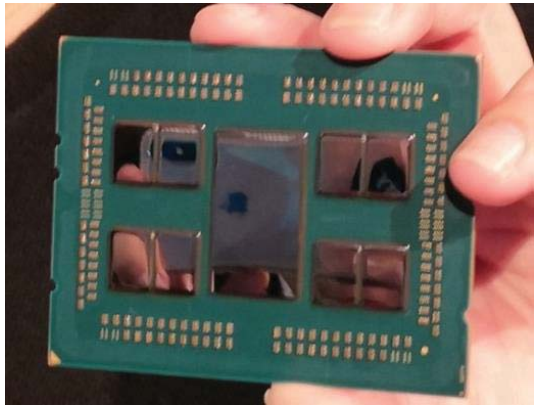
Basics of 2.5D and 3D Integration



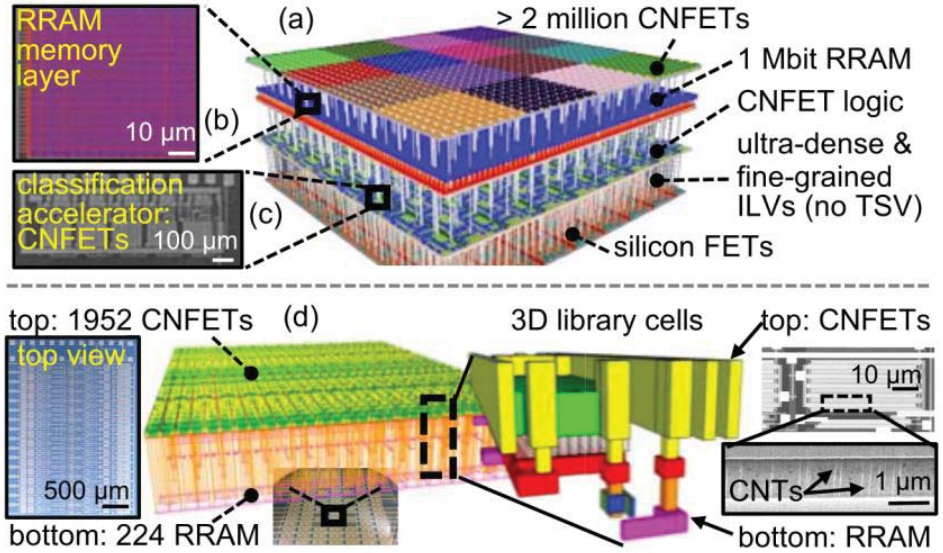
Kim et al., ISSCC, 2012







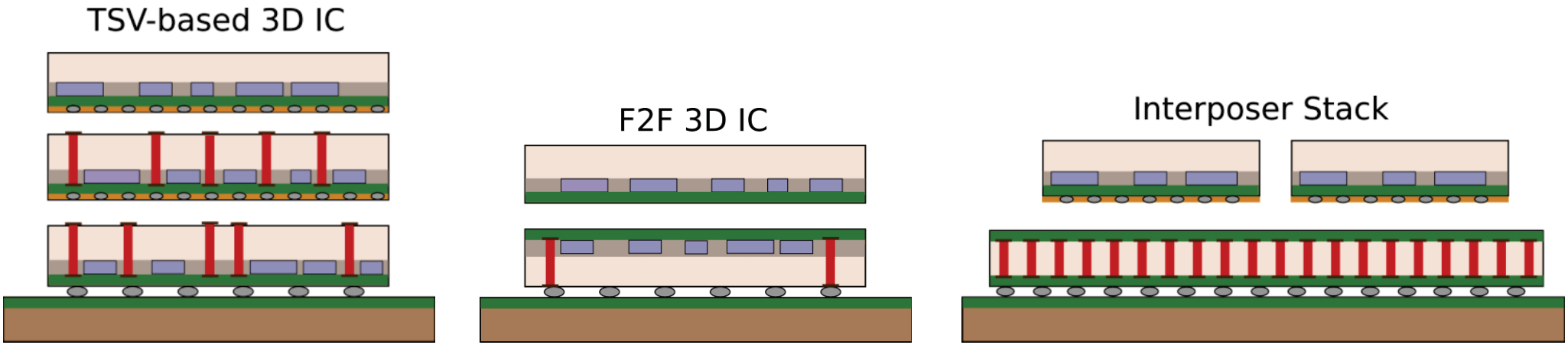
https://www.anandtech.com, 2016 & 2018



Aly et al., Proc. IEEE, 2019

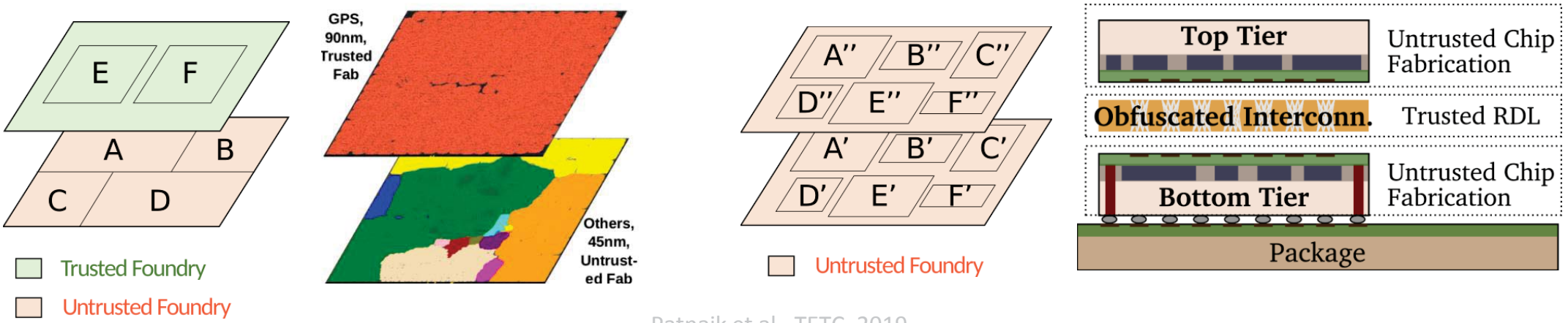
Split Manufacturing with 2.5D and 3D Integration

- **Practical:** FEOL and BEOL processing uninterrupted for separate dies
- **Flexible:** system-level splitting into trusted versus untrusted dies/layers



Split Manufacturing with 2.5D and 3D Integration

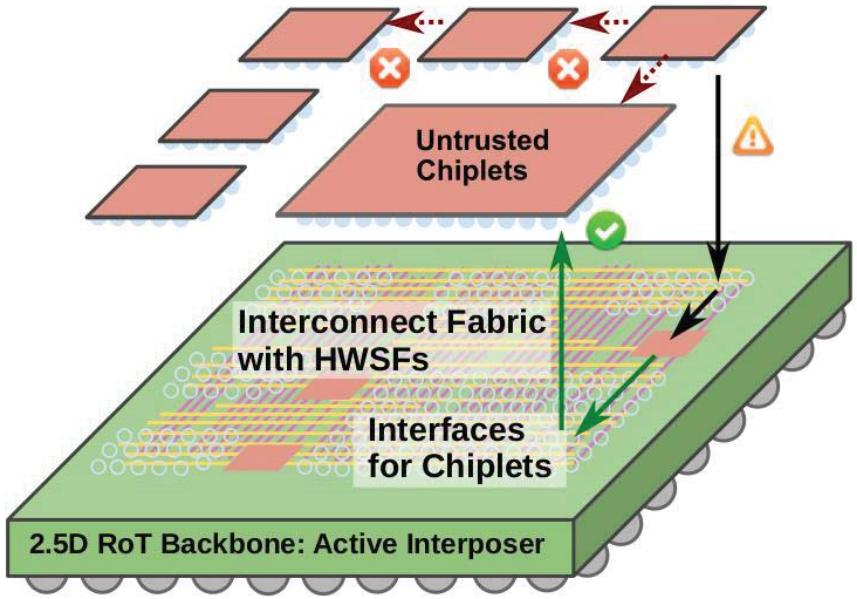
- **Practical:** FEOL and BEOL processing uninterrupted for separate dies
- **Flexible:** system-level splitting into trusted versus untrusted dies/layers
  - E.g., trusted interposer
  - E.g., F2F stacks: one trusted and one untrusted dies, heterogeneous integration; two untrusted dies, trusted RDL in between

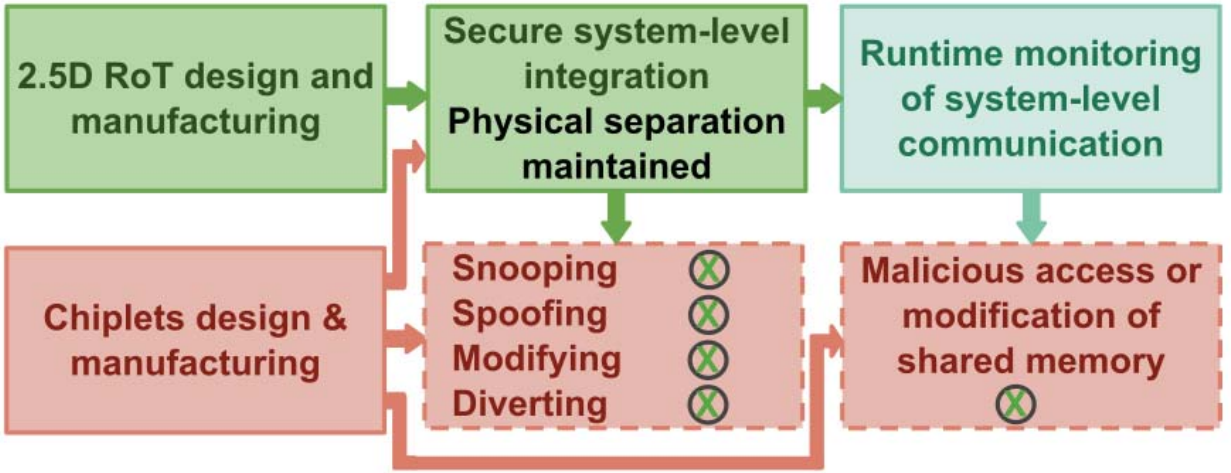


Patnaik et al., TETC, 2019

2.5D and 3D Integration for Hardware Security: Root of Trust

- **Physically secure** system-level integration and runtime monitoring of untrusted chips

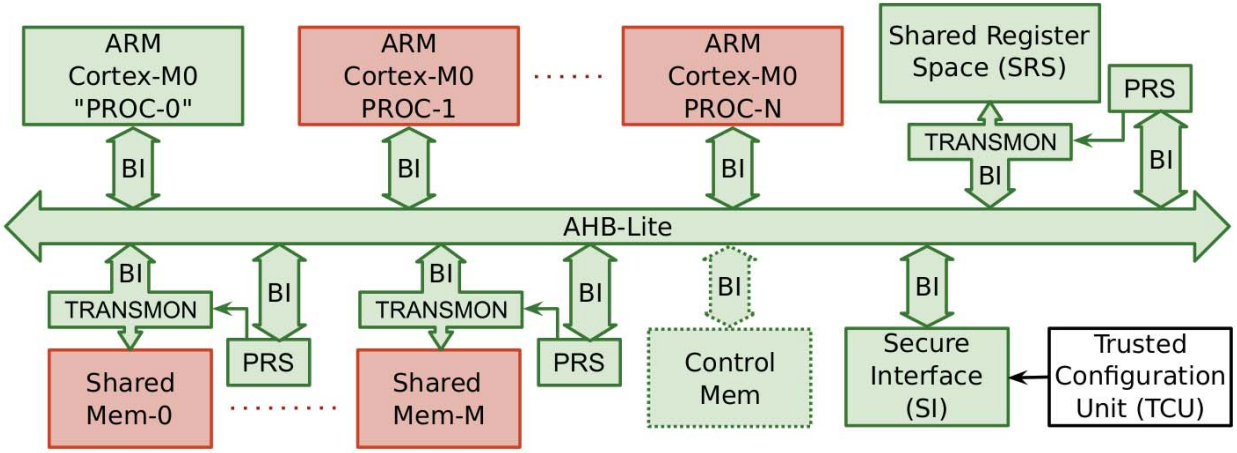




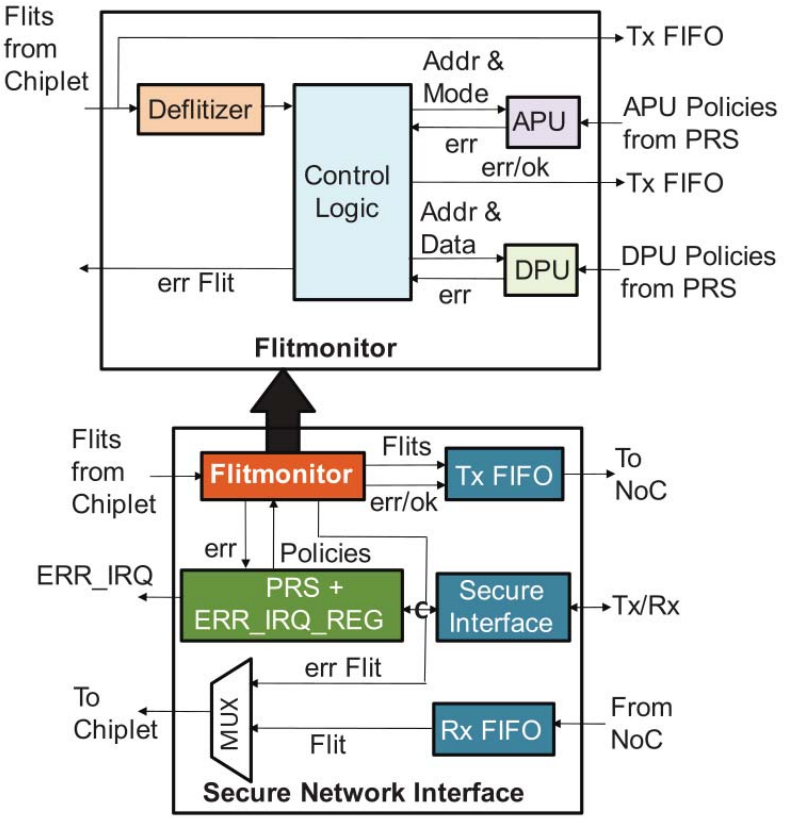
Nabeel et al., TC, 2020

2.5D and 3D Integration for Hardware Security: Root of Trust

- **Physically secure** system-level integration and runtime monitoring of untrusted chips
- Generic principle; demonstrated in an ARM w/ AHBL and a RISC-V w/ NoC architecture



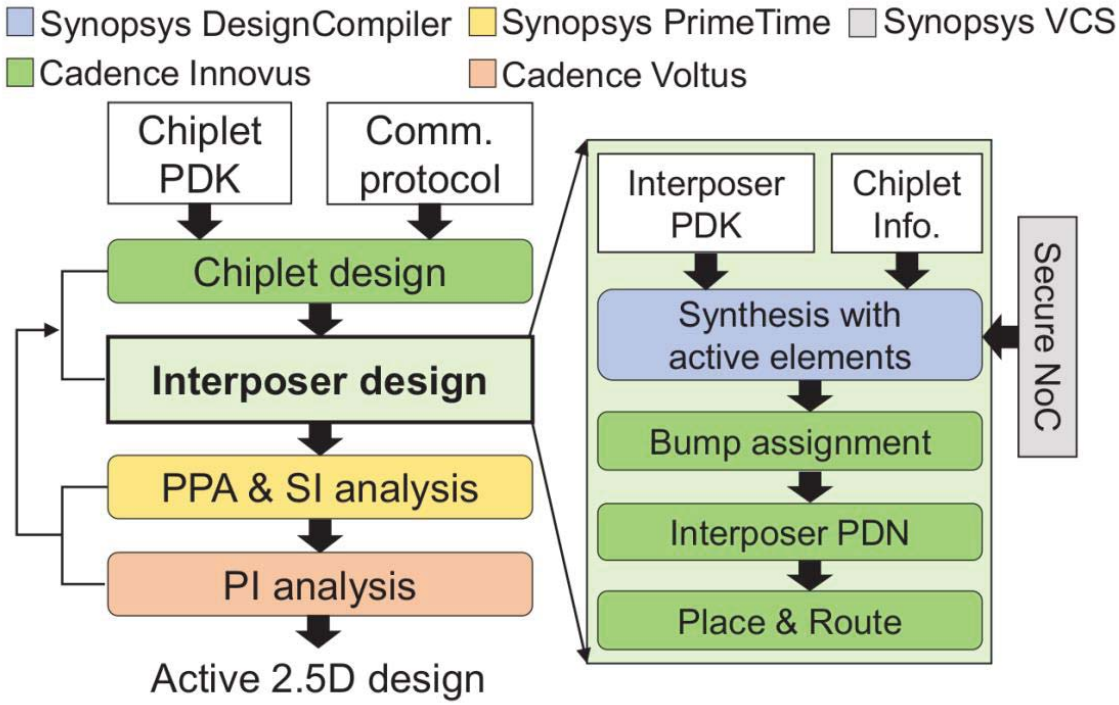
Nabeel et al., TC, 2020

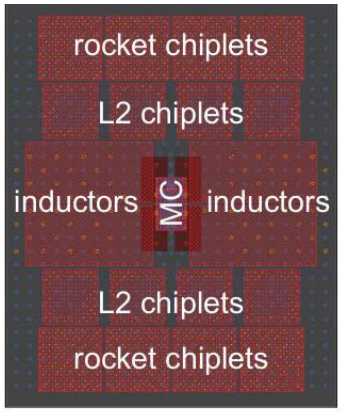


Park et al., TCPMT, 2020

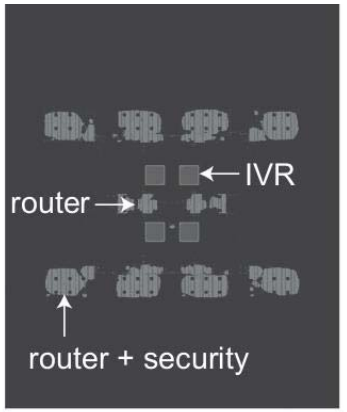
2.5D and 3D Integration for Hardware Security: Root of Trust

- **Physically secure** system-level integration and runtime monitoring of untrusted chips
- Security features easy to integrate in CAD flow

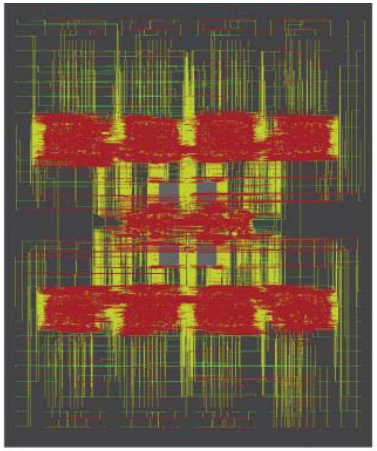




(c) floorplan



(d) interposer placement



(e) interposer routing

Park et al., TCPMT, 2020

Hardware Security for and beyond CMOS Technology: Challenges

- Hardware security relies on technology exploration, device characterization, circuit design, architectures, etc.
  → CAD support for security schemes as well as emerging technologies is essential

- Closer interaction between communities: security, technology, CAD
  → Joint (re-)definition and application of security metrics across the stack
  → Joint (re-)consideration of threat models
  → Technology exploration with early focus on security, not as after-thought

- Most emerging technologies are CMOS compatible/hybrid
  → System-level identification of “weakest link” in security scheme

wp.nyu.edu/johann **Thank you!** **johann@nyu.edu**