جامعة نيويورك أبوظبي
NYU ABU DHABI

CENTER FOR CYBER SECURITY

DFX LAB
DESIGN FOR EXCELLENCE

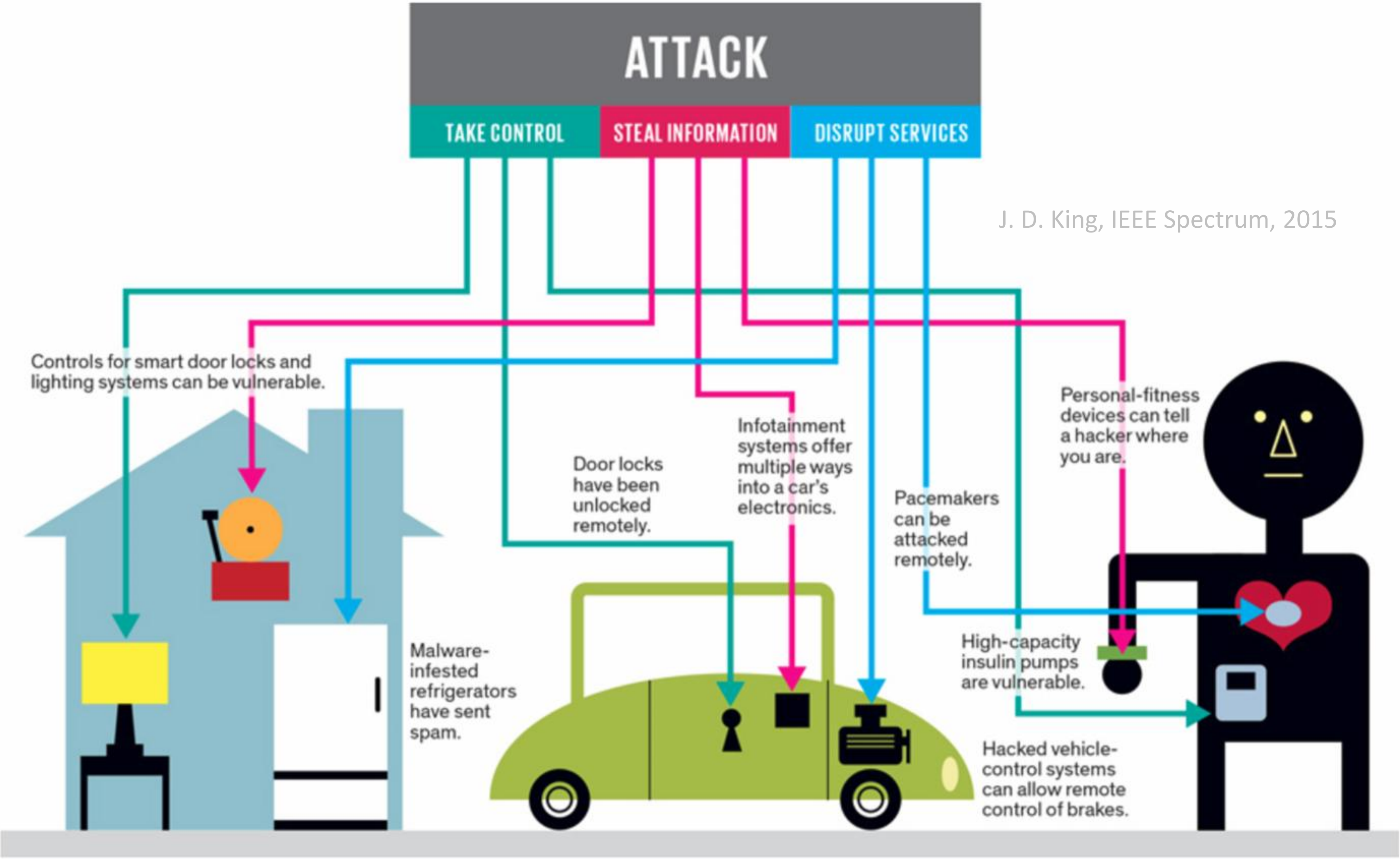
Hardware Security for and beyond CMOS Technology

Johann Knechtel

johann@nyu.edu

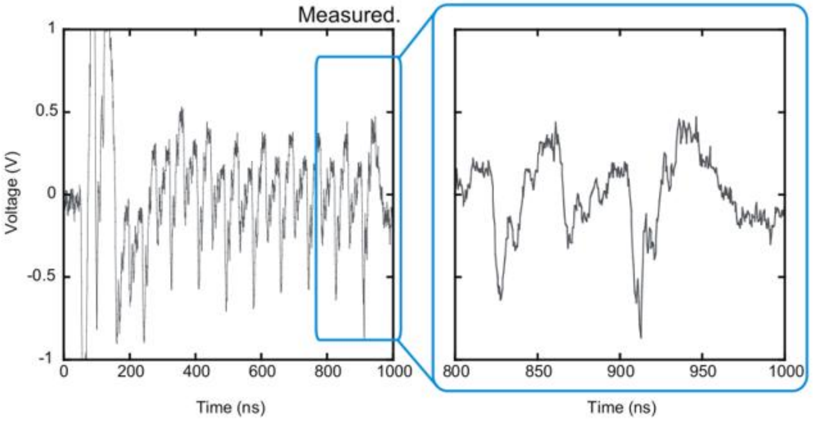
wp.nyu.edu/johann   arxiv.org/abs/2001.08780

CESG Seminar at TAMU – Oct 2, 2020

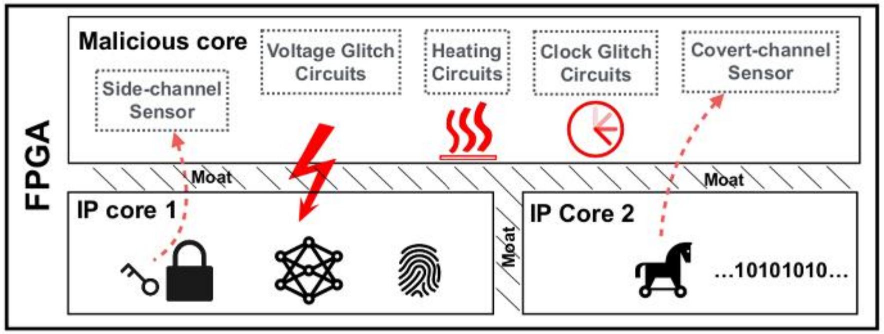

ATTACK
TAKE CONTROL
STEAL INFORMATION
DISRUPT SERVICES
Controls for smart door locks and lighting systems can be vulnerable.
Malware-infested refrigerators have sent spam.
Door locks have been unlocked remotely.
Infotainment systems offer multiple ways into a car's electronics.
Pacemakers can be attacked remotely.
Personal-fitness devices can tell a hacker where you are.
High-capacity insulin pumps are vulnerable.
Hacked vehicle-control systems can allow remote control of brakes.

J. D. King, IEEE Spectrum, 2015

Data and Computation at Risk – Right at the Hardware



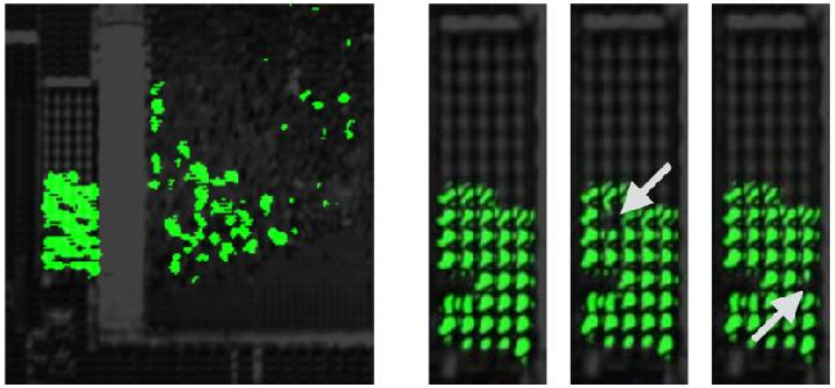
Fujimoto et al., EMC 2014



Alam et al., FDTC 2019

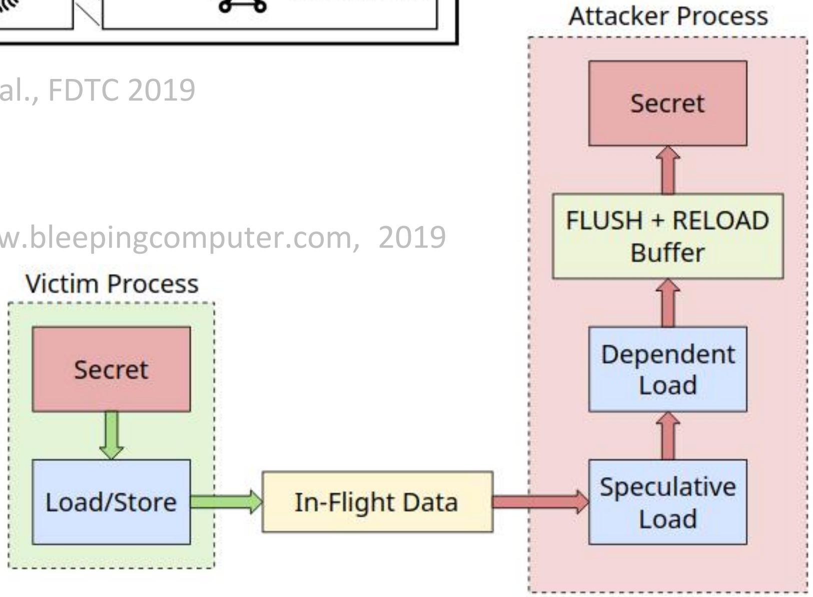
MELTDOWN

SPECTRE



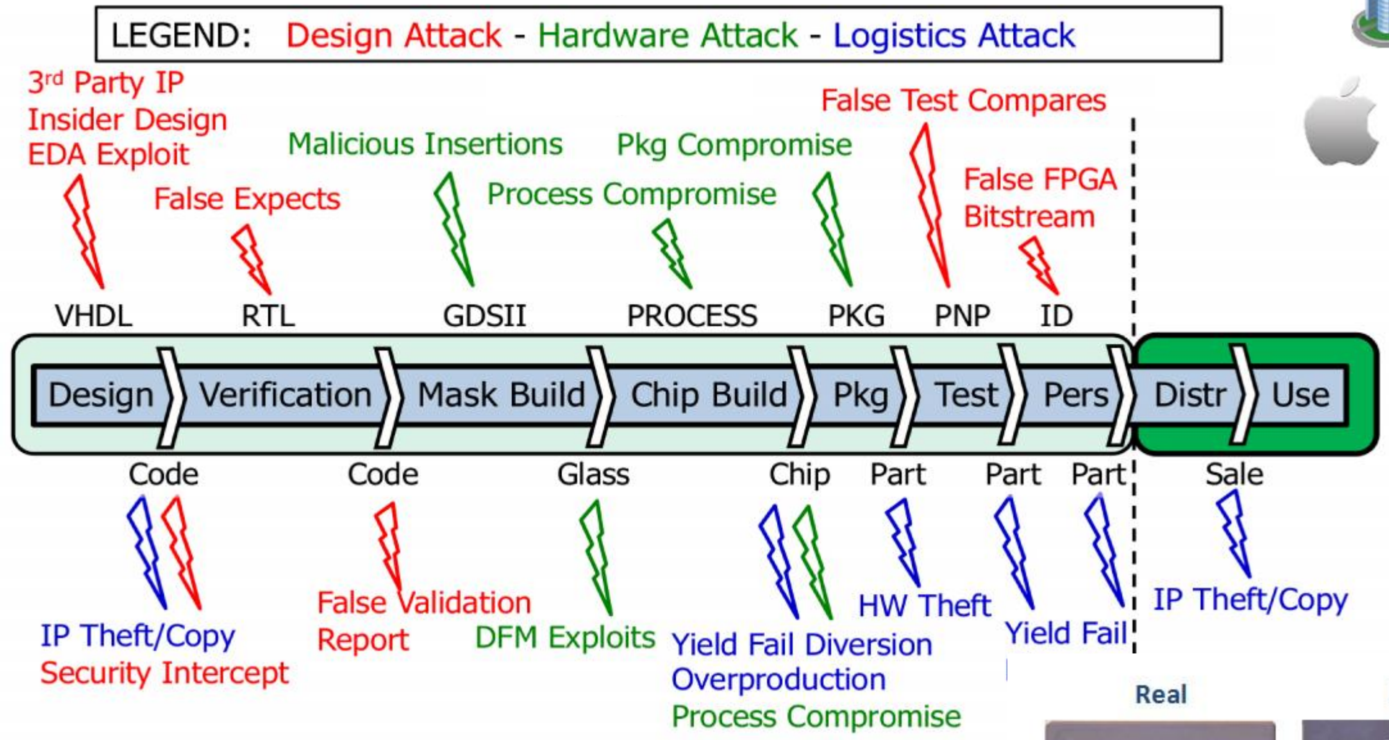
Tajik et al., CCS, 2017

MD S

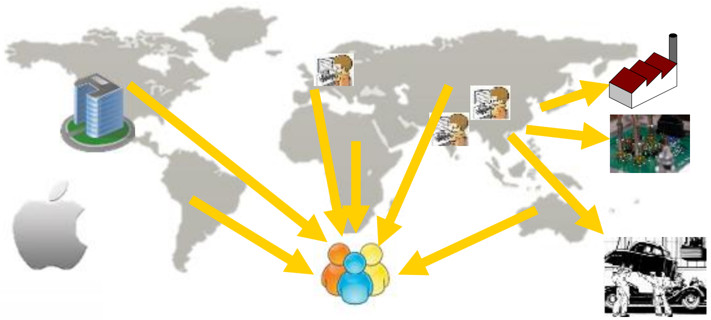


https://www.bleepingcomputer.com, 2019

Hardware Itself Also at Risk



Kerry Bernstein, DARPA, 2016

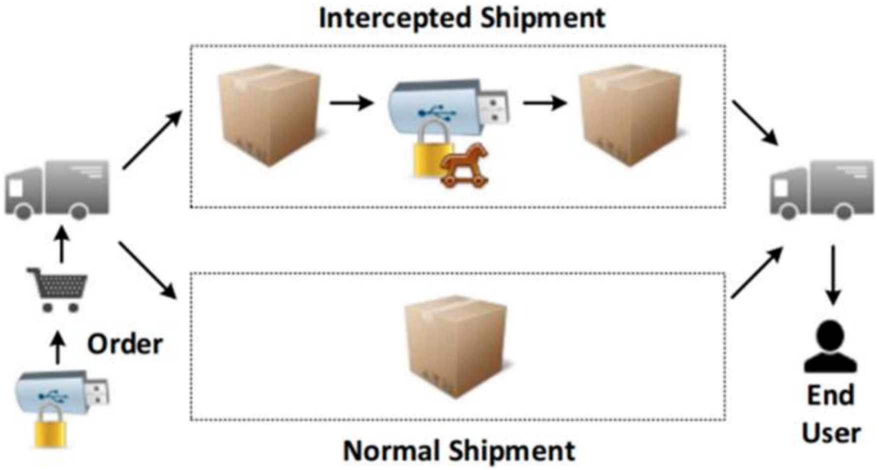


IEEE Spectrum, 2015

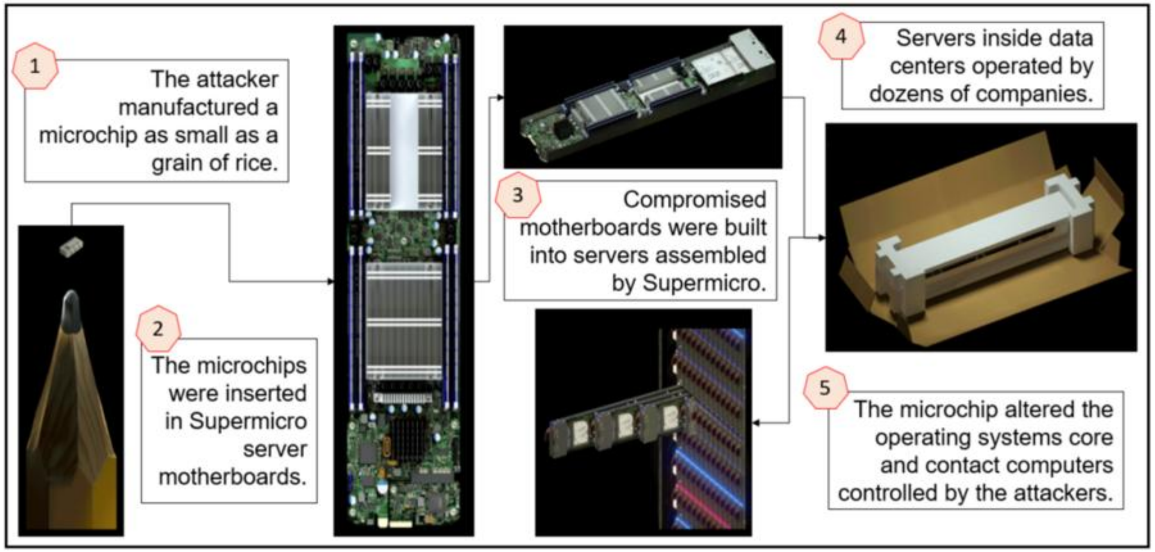
A Note on Trojans

- Unlikely inserted by foundries – fatal business consequences
- More likely:
  - Untrustworthy 3rd party IP
  - Adversarial designers, hacking of design environment
  - Distribution and deployment; see also Snowden papers or “Big Hack”

Mehta et al., JETC, 2020



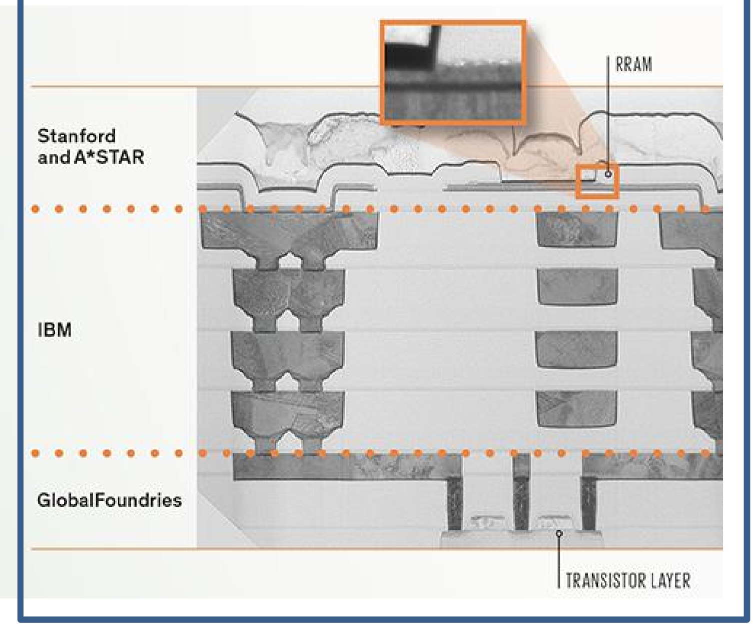
Swierczynski et al., 2017

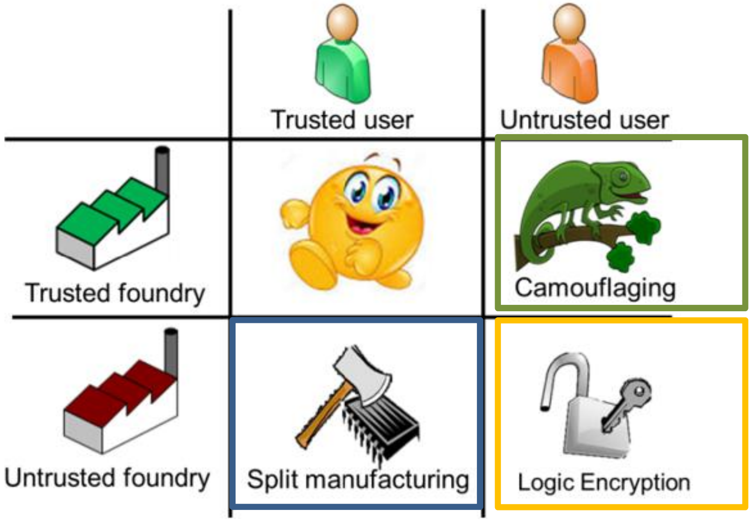

1
The attacker manufactured a microchip as small as a grain of rice.
2
The microchips were inserted in Supermicro server motherboards.
3
Compromised motherboards were built into servers assembled by Supermicro.
4
Servers inside data centers operated by dozens of companies.
5
The microchip altered the operating systems core and contact computers controlled by the attackers.

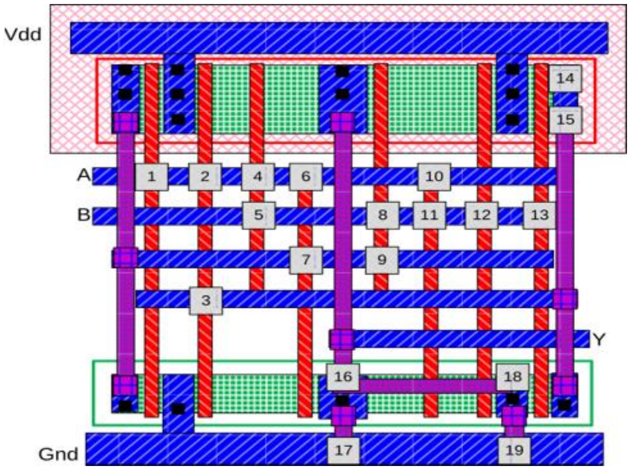
(CMOS) Countermeasures Against Attacks on Hardware

- IP protection

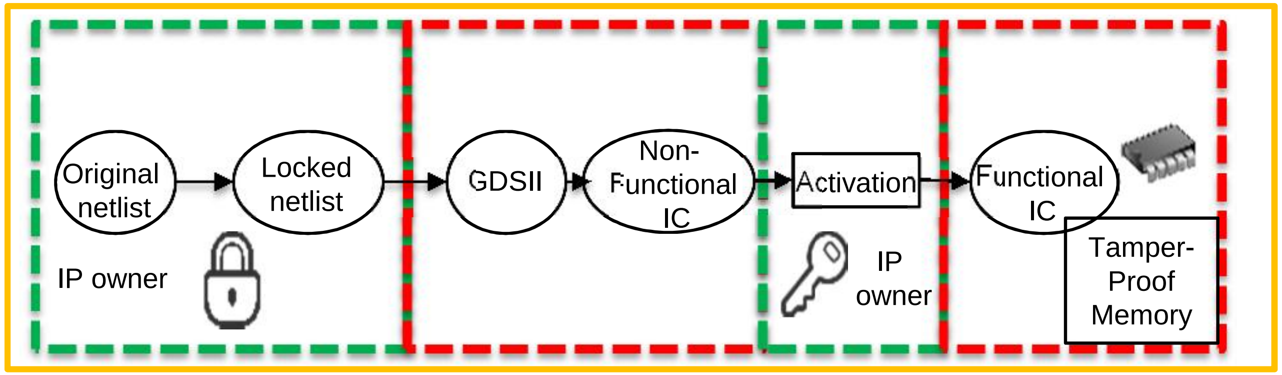
IEEE Spectrum, 2015





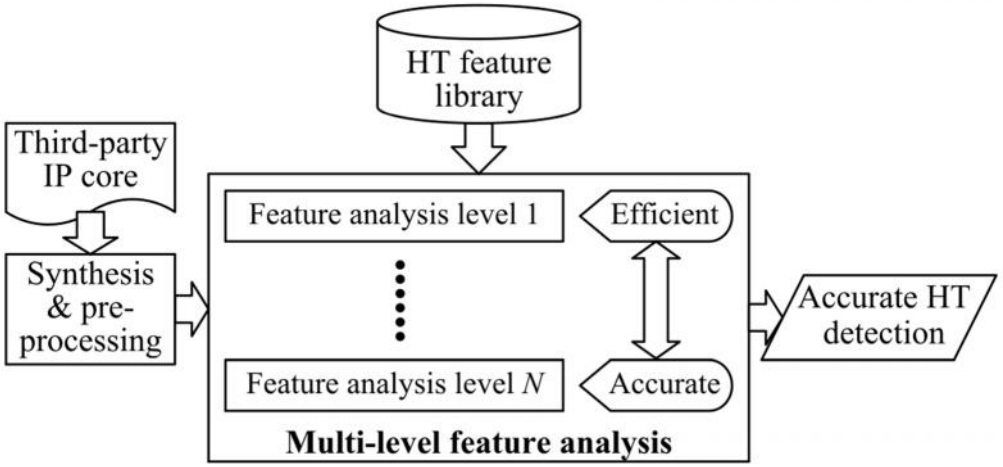


Rajendran et al., CCS, 2013

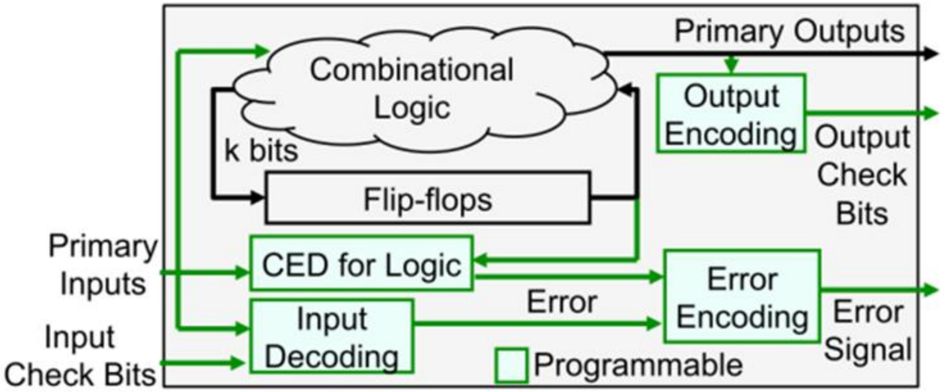


(CMOS) Countermeasures Against Attacks on Hardware

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



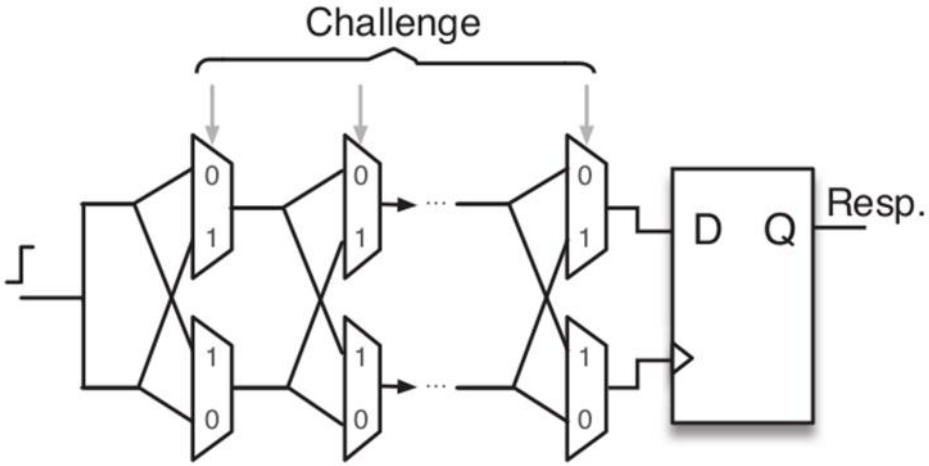
Chen et al., TCAD 2018



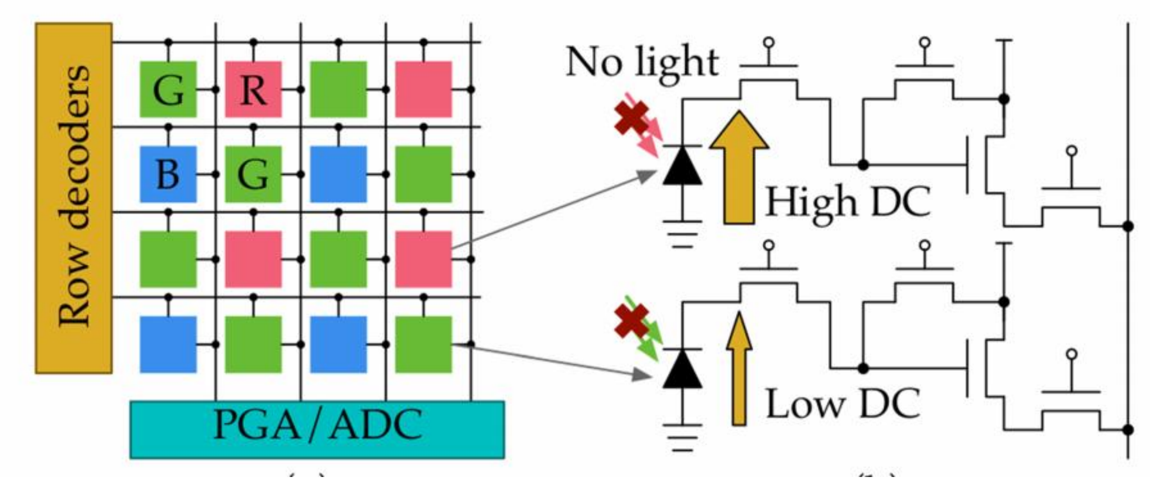
Wu et al., TCAD 2016

(CMOS) Countermeasures Against Attacks on Hardware

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



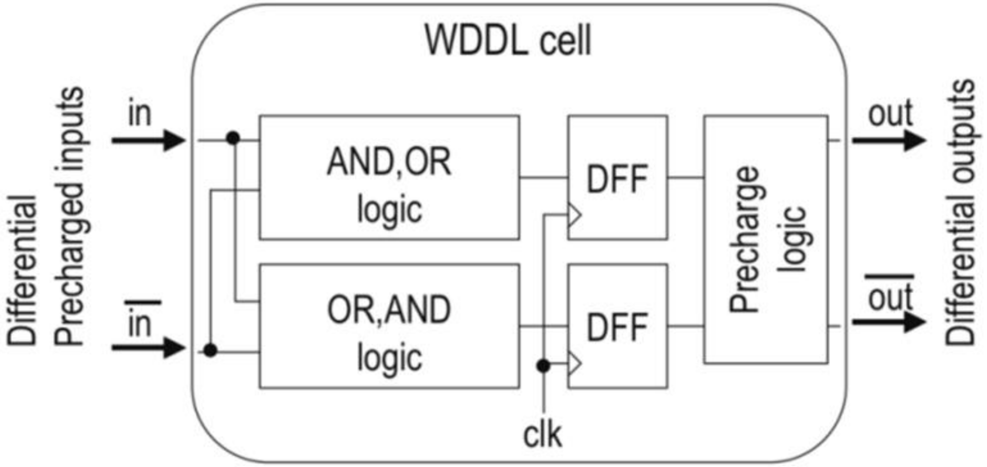
Vatajelu19, IOLTS, 2019



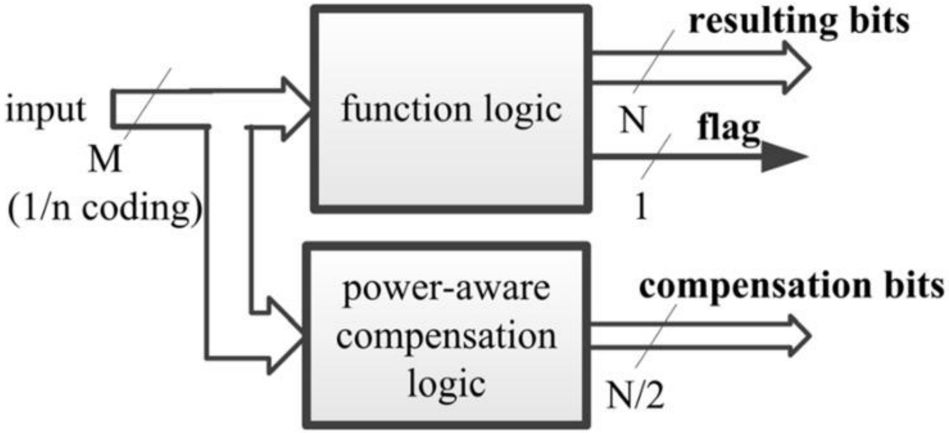
Kim and Lee, DAC, 2018

(CMOS) Countermeasures Against Runtime Attacks

- Masking against side-channel attacks



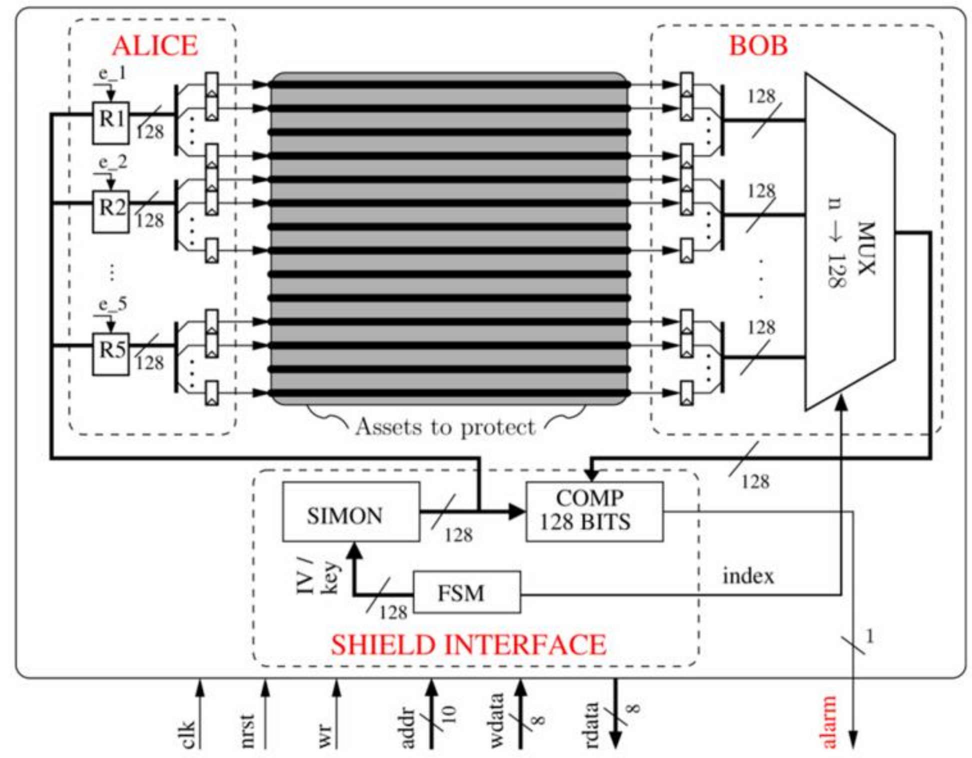
Fujimoto et al., EMC 2014



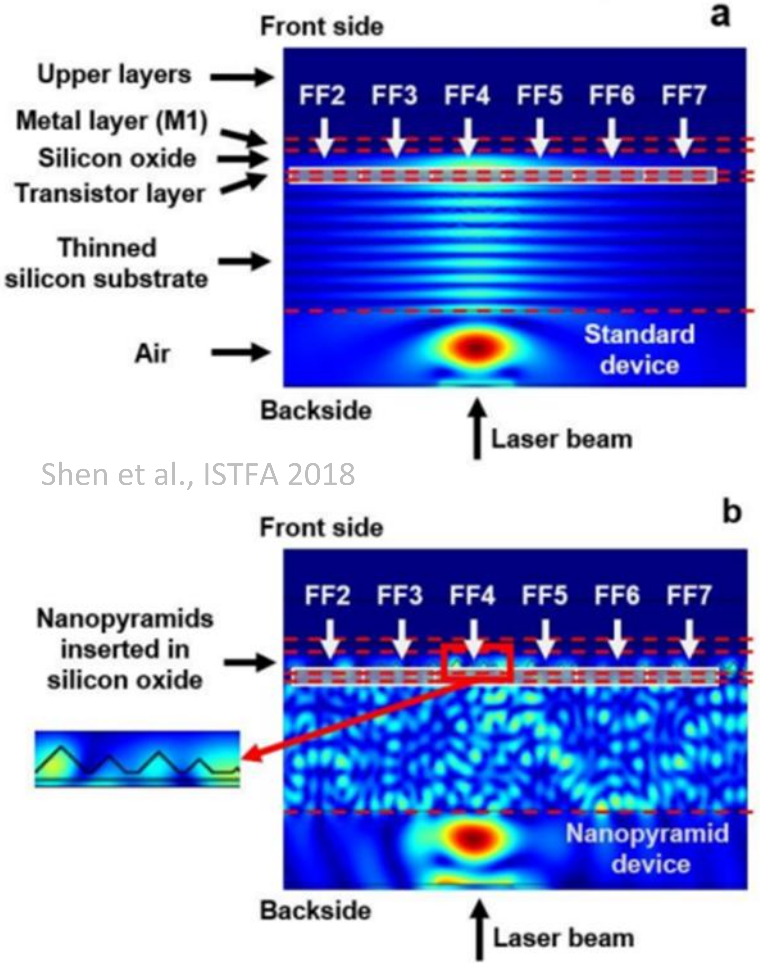
Li et al., TVLSI 2017

(CMOS) Countermeasures Against Runtime Attacks

- Masking against side-channel attacks
- Shielding against probing (front side, back side)

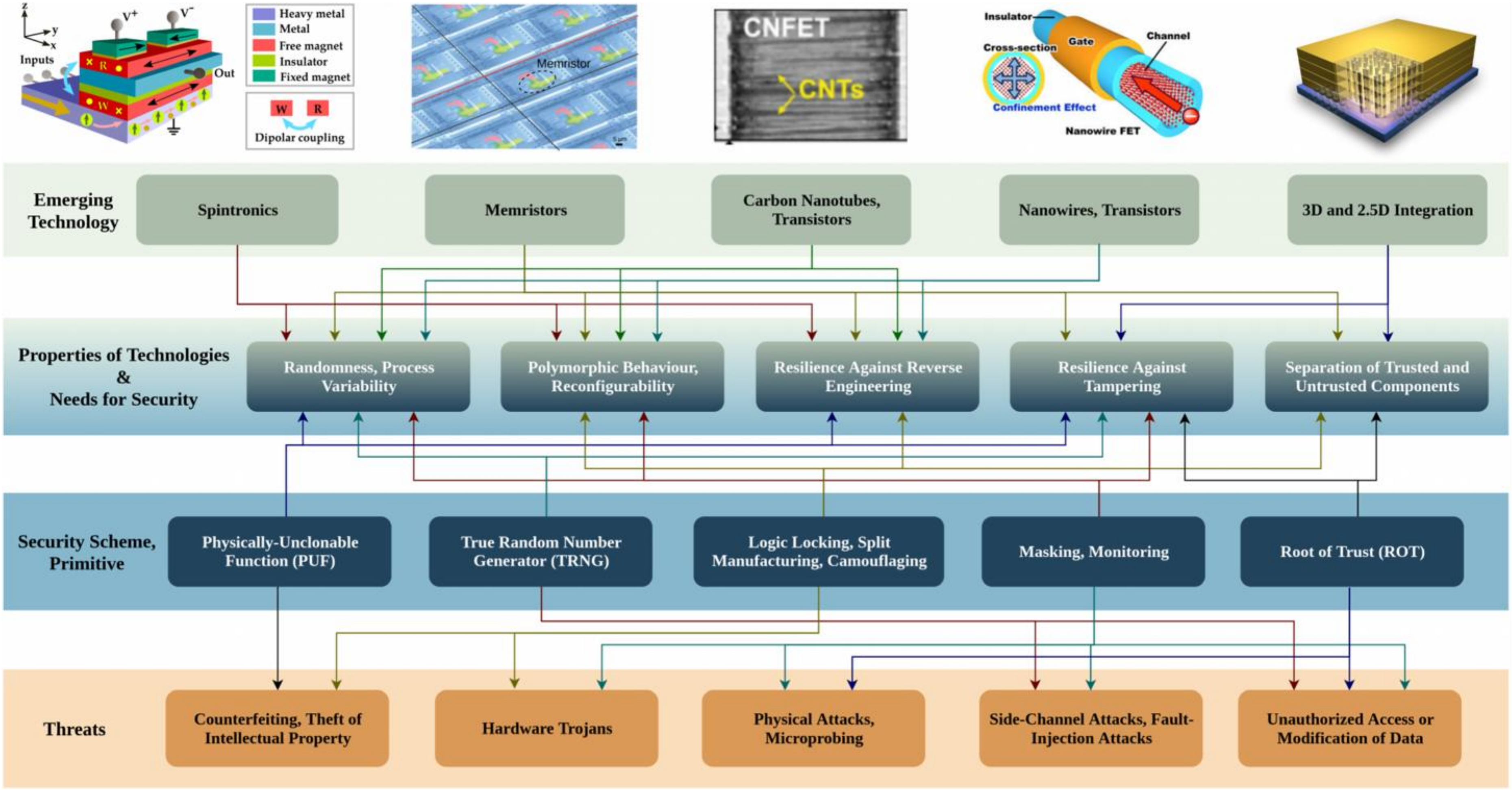


Ngo et al., TC 2017



Shen et al., ISTFA 2018

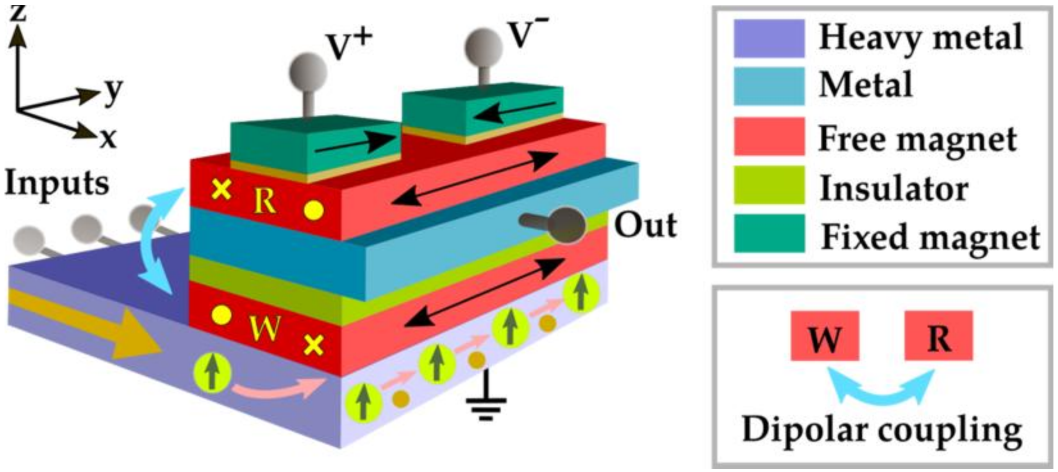
Beyond-CMOS Technologies for Hardware Security



Emerging Technology	Spintronics	Memristors	Carbon Nanotubes, Transistors	Nanowires, Transistors	3D and 2.5D Integration
Properties of Technologies & Needs for Security	Randomness, Process Variability	Polymorphic Behaviour, Reconfigurability	Resilience Against Reverse Engineering	Resilience Against Tampering	Separation of Trusted and Untrusted Components
Security Scheme, Primitive	Physically-Unclonable Function (PUF)	True Random Number Generator (TRNG)	Logic Locking, Split Manufacturing, Camouflaging	Masking, Monitoring	Root of Trust (ROT)
Threats	Counterfeiting, Theft of Intellectual Property	Hardware Trojans	Physical Attacks, Microprobing	Side-Channel Attacks, Fault-Injection Attacks	Unauthorized Access or Modification of Data

Basics of Spintronics

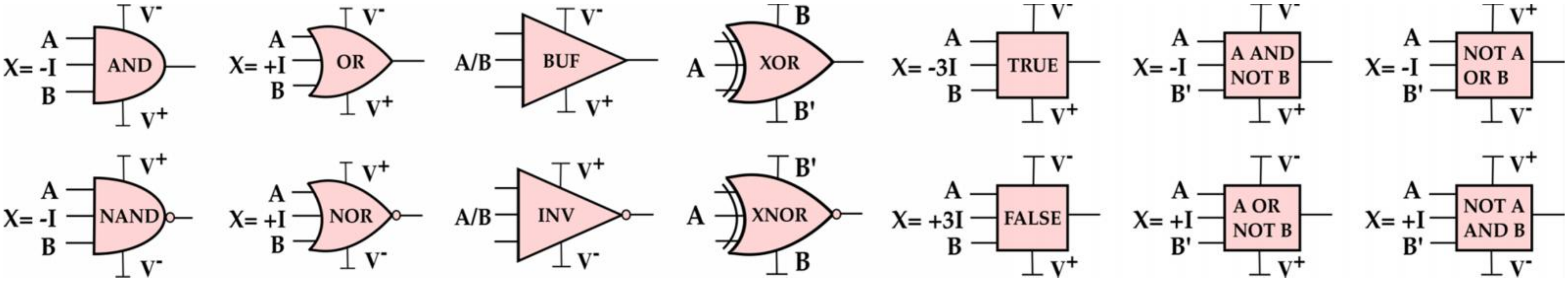
- Besides electronic charge, *spin* of electrons is leveraged for computation and memory
- Switching process is non-volatile, magnetoelectric, and subject to phenomena like spin-transfer torque (STT)
- Implemented typically as stack of heavy metals, ferromagnets, or oxide structures – can be made compatible with CMOS



Patnaik et al., TCAD 2019

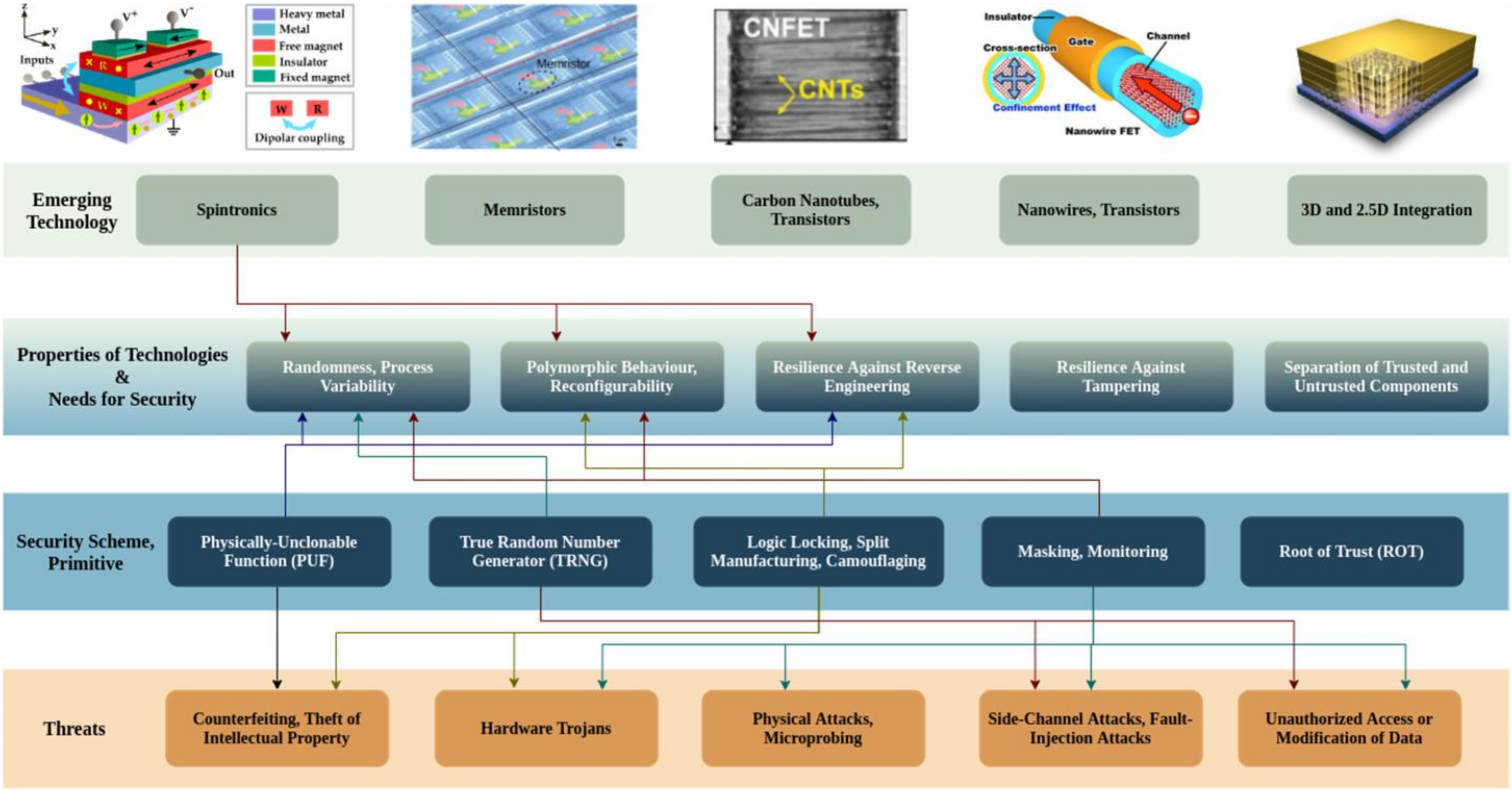
Basics of Spintronics

- In comparison to CMOS, spintronic devices 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



Emerging Technology

Spintronics

Memristors

Carbon Nanotubes, Transistors

Nanowires, Transistors

3D and 2.5D Integration

Properties of Technologies & Needs for Security

Randomness, Process Variability

Polymorphic Behaviour, Reconfigurability

Resilience Against Reverse Engineering

Resilience Against Tampering

Separation of Trusted and Untrusted Components

Security Scheme, Primitive

Physically-Unclonable Function (PUF)

True Random Number Generator (TRNG)

Logic Locking, Split Manufacturing, Camouflaging

Masking, Monitoring

Root of Trust (ROT)

Threats

Counterfeiting, Theft of Intellectual Property

Hardware Trojans

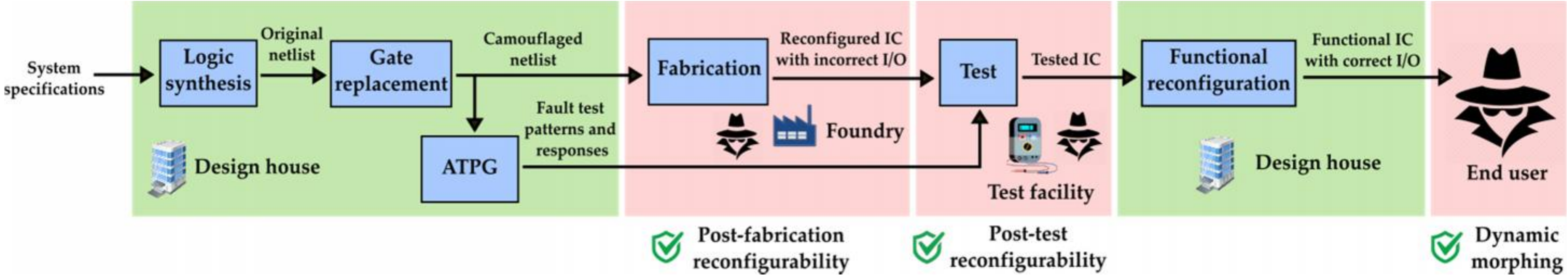
Physical Attacks, Microprobing

Side-Channel Attacks, Fault-Injection Attacks

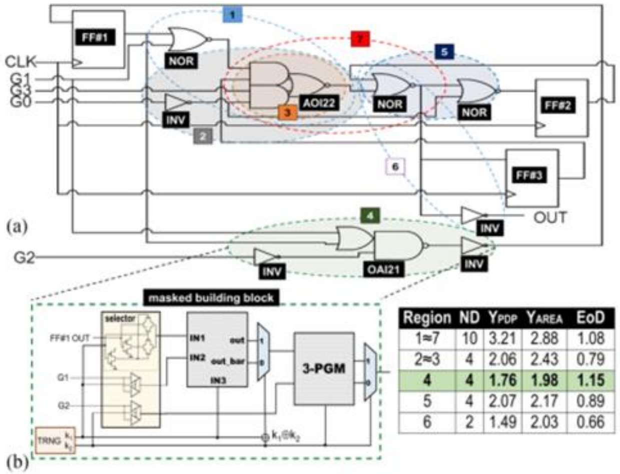
Unauthorized Access or Modification of Data

Spintronics for Hardware Security

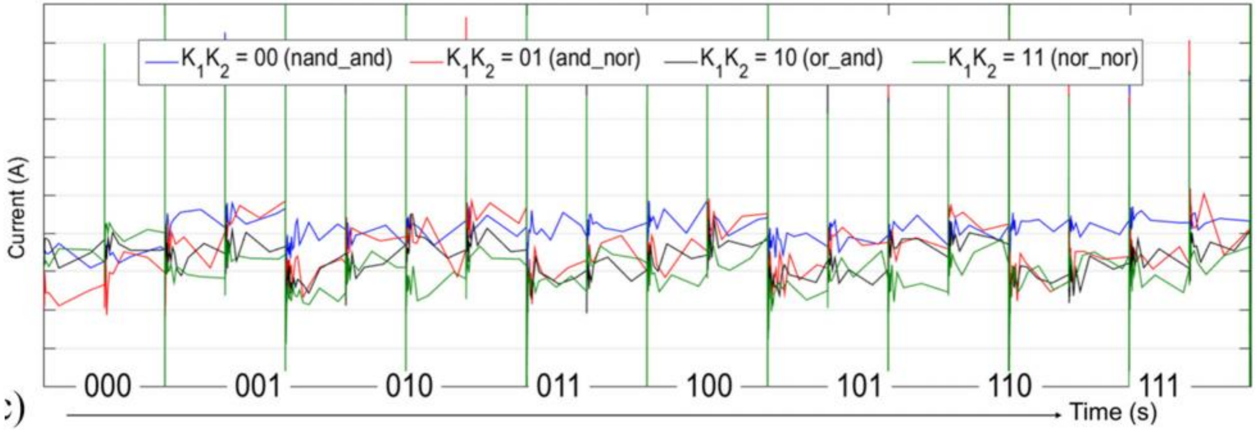
- Dynamic camouflaging as novel paradigm for IP protection
- Polymorphic switching, non-CMOS switching mechanism to mitigate side-channel leakage


System specifications
Logic synthesis
Original netlist
Gate replacement
Camouflaged netlist
ATPG
Fault test patterns and responses
Design house
Fabrication
Reconfigured IC with incorrect I/O
Foundry
Test
Tested IC
Test facility
Functional reconfiguration
Functional IC with correct I/O
Design house
End user
Post-fabrication reconfigurability
Post-test reconfigurability
Dynamic morphing

Rangarajan et al., ^TETC, 2020



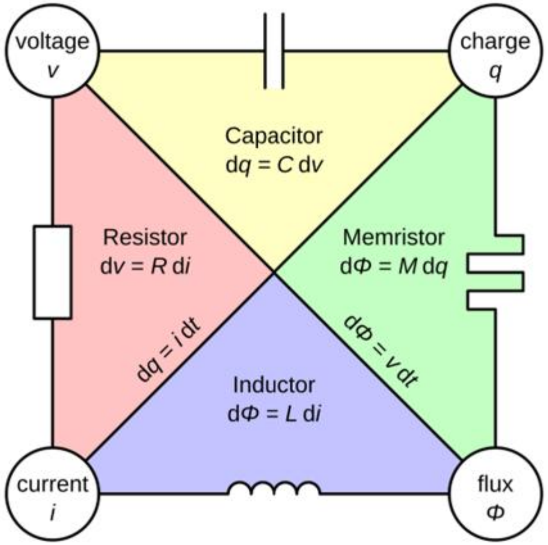
Region	ND	Y_{PDP}	Y_{AREA}	EoD
1≈7	10	3.21	2.88	1.08
2≈3	4	2.06	2.43	0.79
4	**4**	**1.76**	**1.98**	**1.15**
5	4	2.07	2.17	0.89
6	2	1.49	2.03	0.66

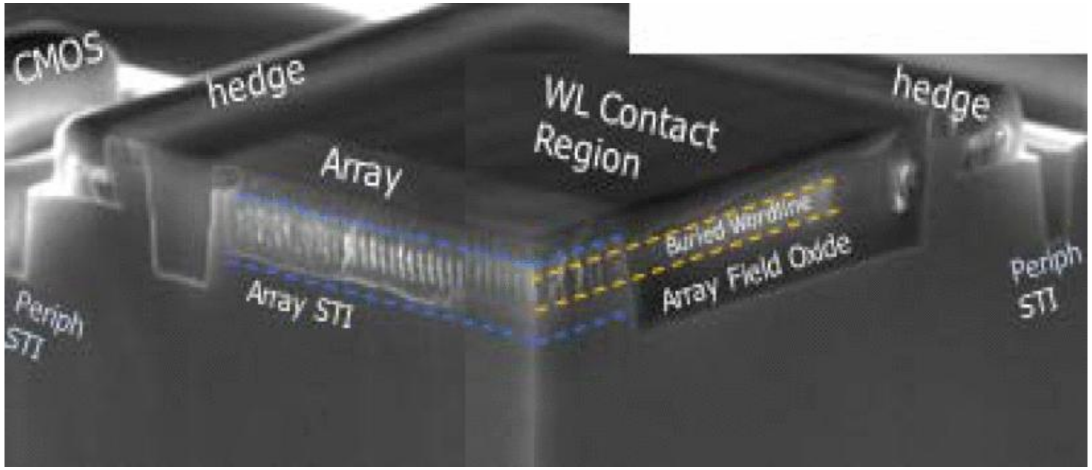


Roohi et al., TNANO, 2019

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

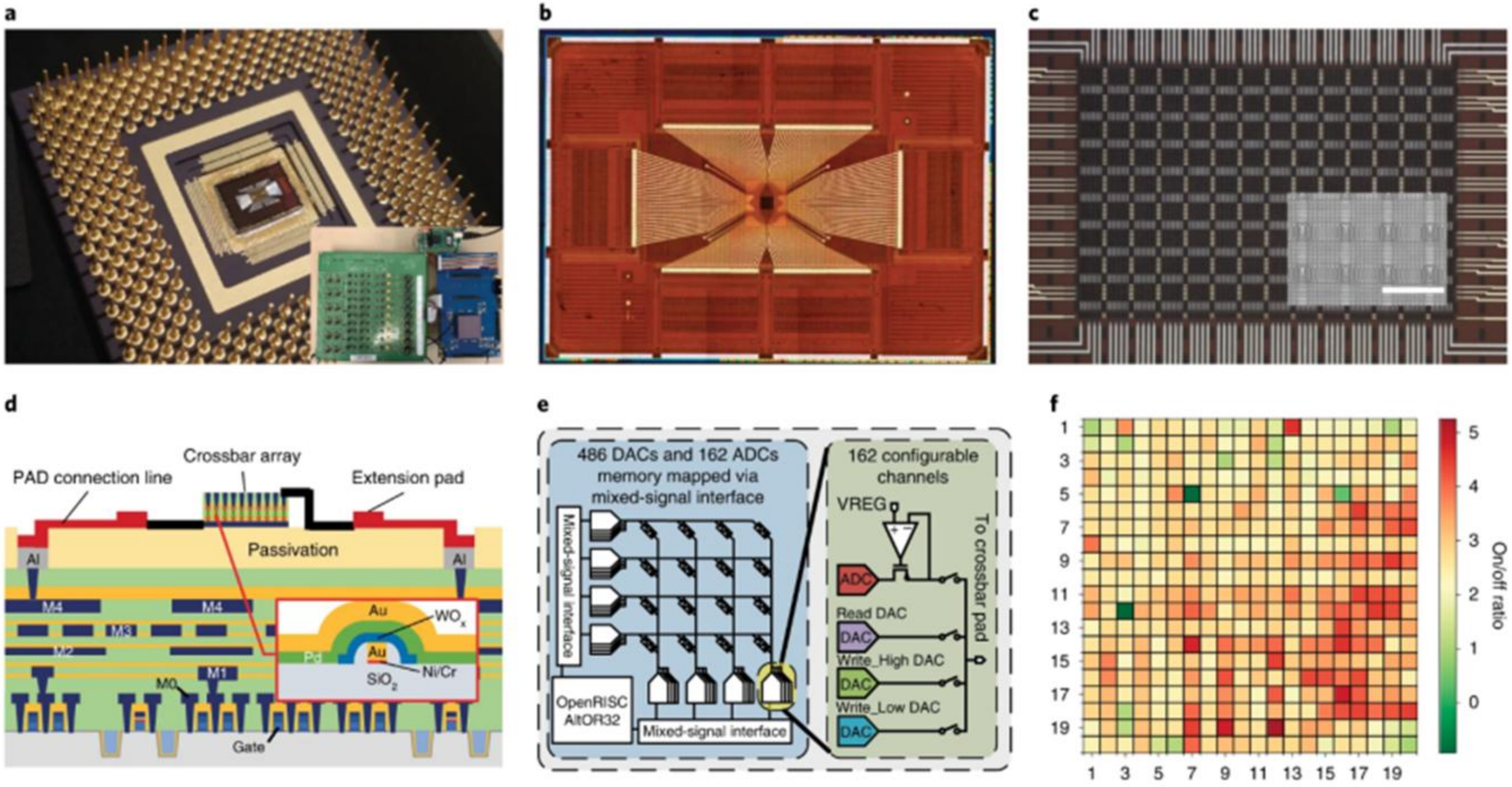




Zahurak et al., IEDM 2014

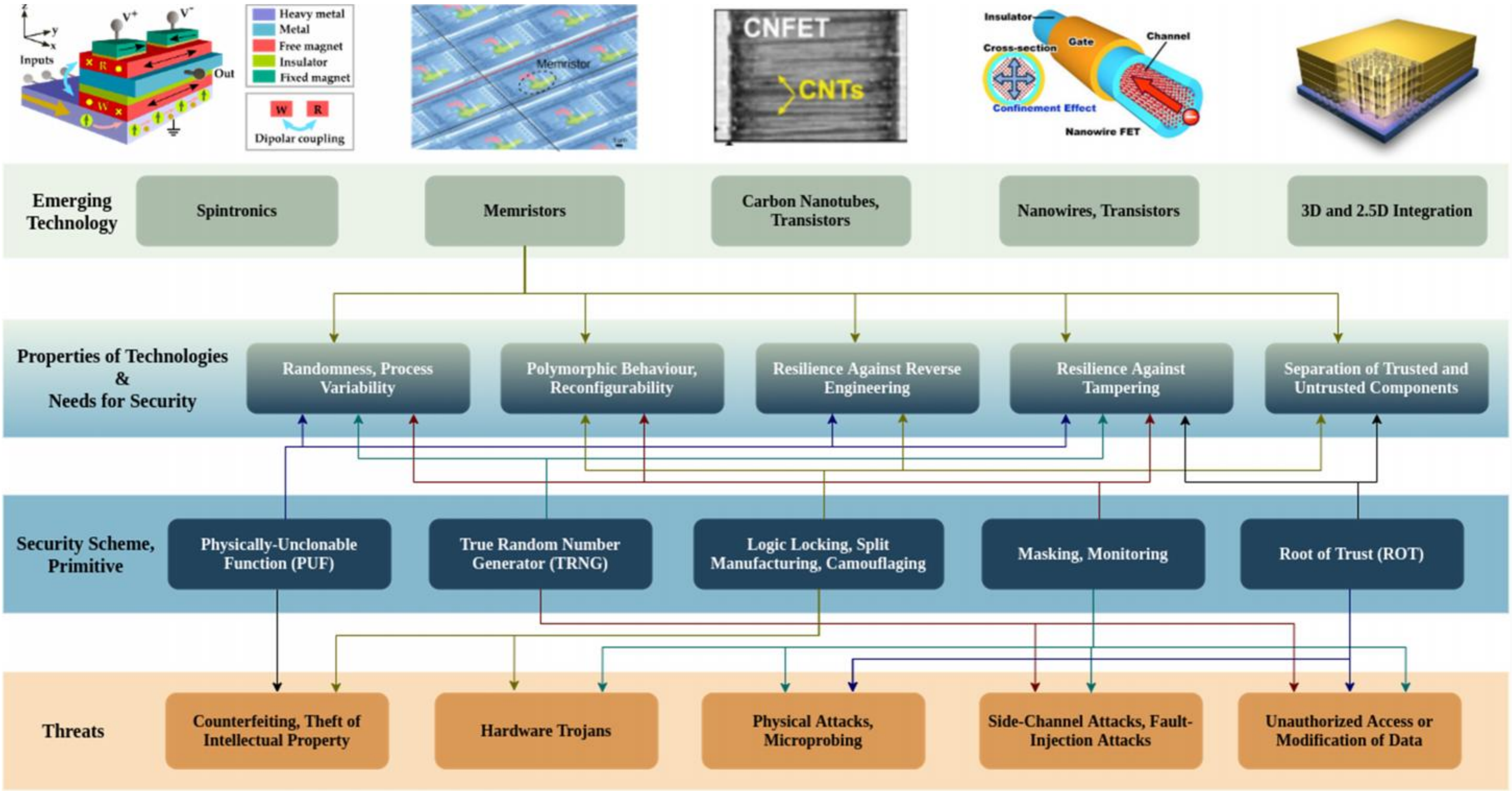
Basics of Memristors

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



Cai et al., Nature 2019

Memristors for Hardware Security



Emerging Technology

Spintronics

Memristors

Carbon Nanotubes, Transistors

Nanowires, Transistors

3D and 2.5D Integration

Properties of Technologies & Needs for Security

Randomness, Process Variability

Polymorphic Behaviour, Reconfigurability

Resilience Against Reverse Engineering

Resilience Against Tampering

Separation of Trusted and Untrusted Components

Security Scheme, Primitive

Physically-Unclonable Function (PUF)

True Random Number Generator (TRNG)

Logic Locking, Split Manufacturing, Camouflaging

Masking, Monitoring

Root of Trust (ROT)

Threats

Counterfeiting, Theft of Intellectual Property

Hardware Trojans

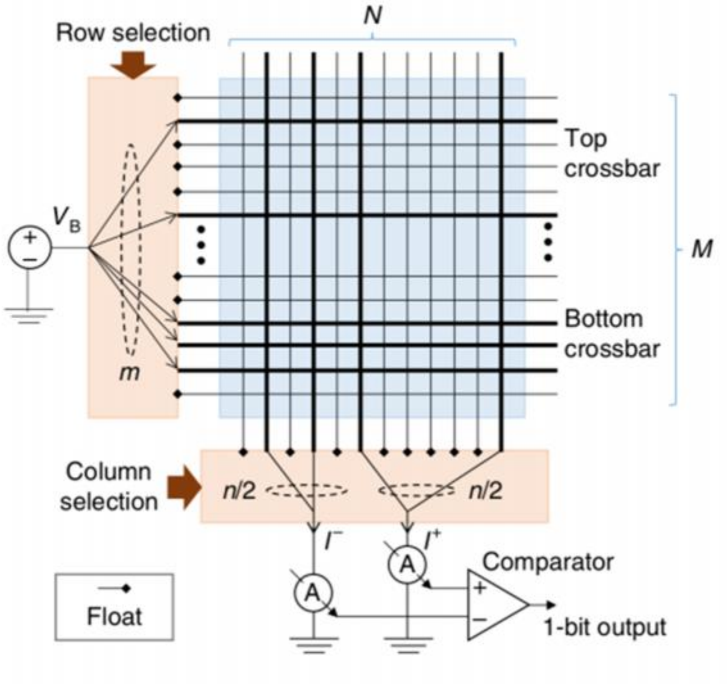
Physical Attacks, Microprobing

Side-Channel Attacks, Fault-Injection Attacks

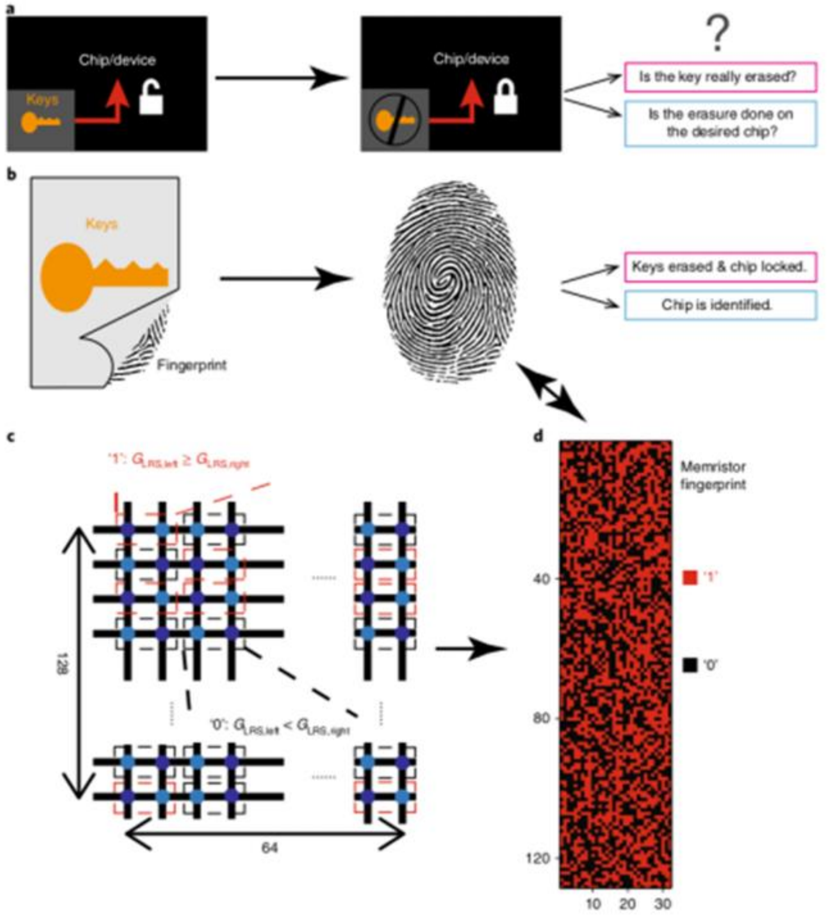
Unauthorized Access or Modification of Data

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



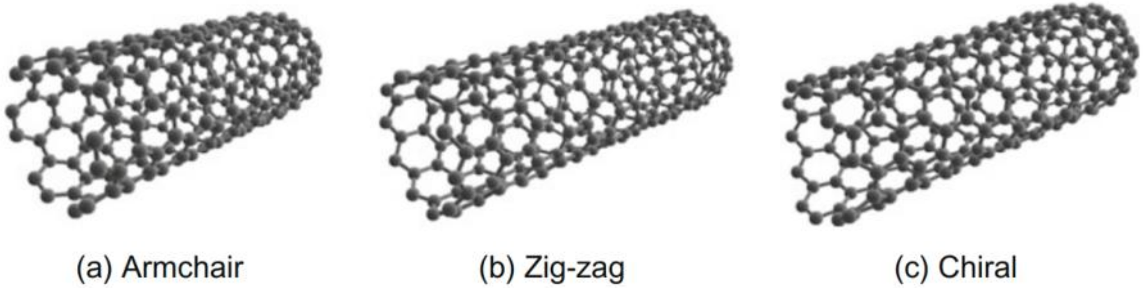
Nili et al., Nature 2018


a
Chip/device
Keys
Chip/device
?
Is the key really erased?
Is the erasure done on the desired chip?
b
Keys
Fingerprint
Keys erased & chip locked.
Chip is identified.
c
'1': $G_{LRS,left} \geq G_{LRS,right}$
128
'0': $G_{LRS,left} < G_{LRS,right}$
64
d
Memristor fingerprint
'1'
'0'
40
80
120
10
20
30

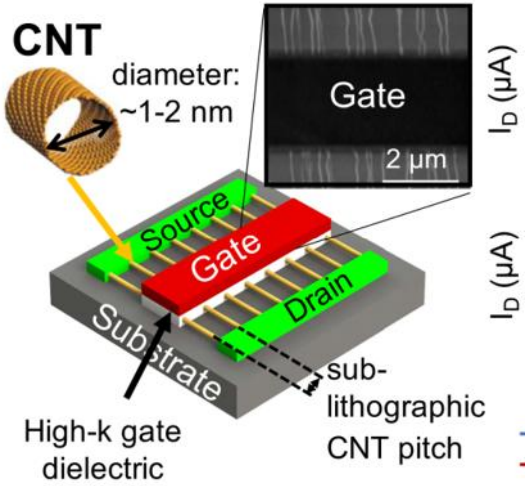
Jiang et al., Nature 2018

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

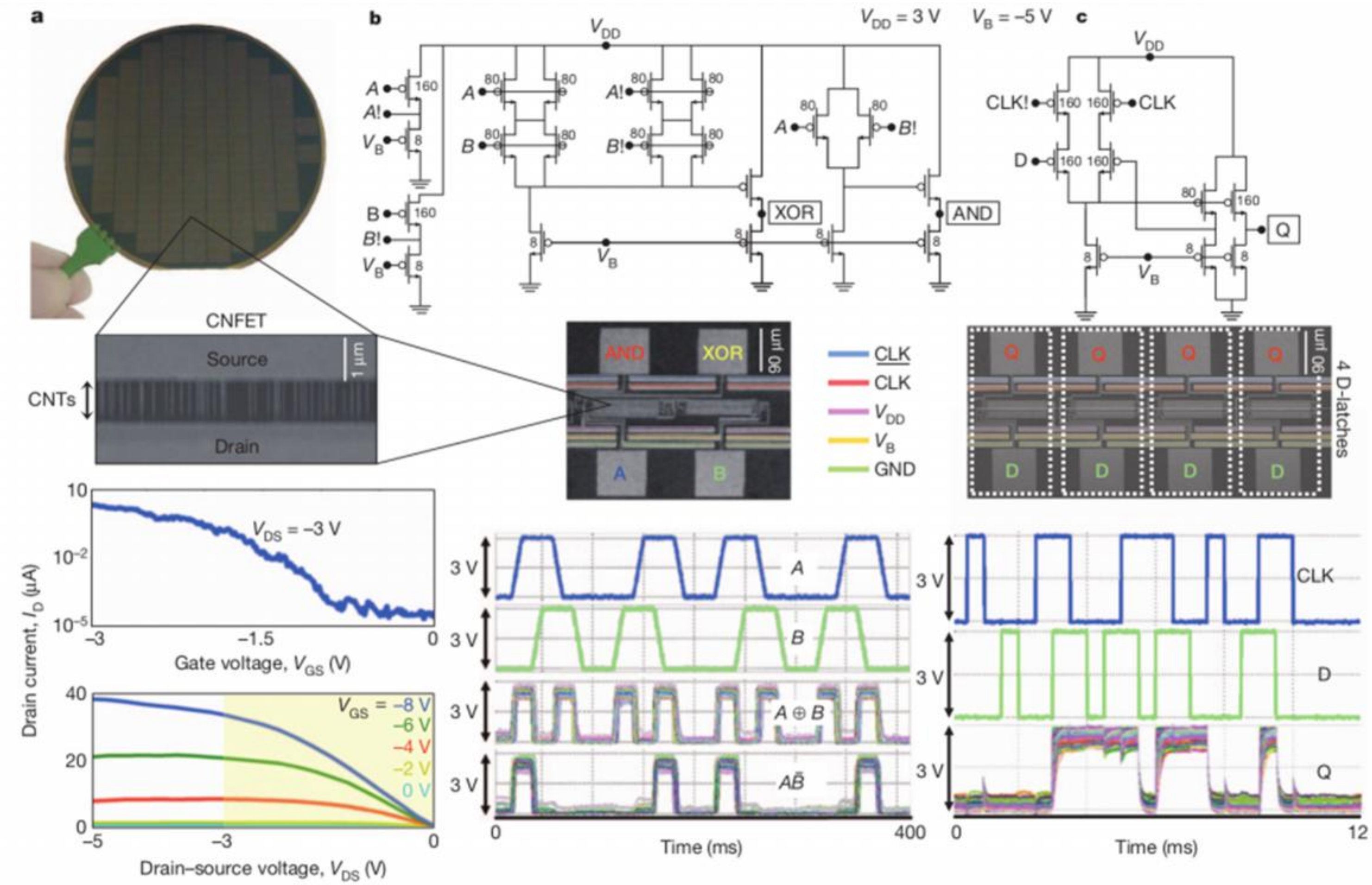


Lienig and Thiele, Springer, 2018



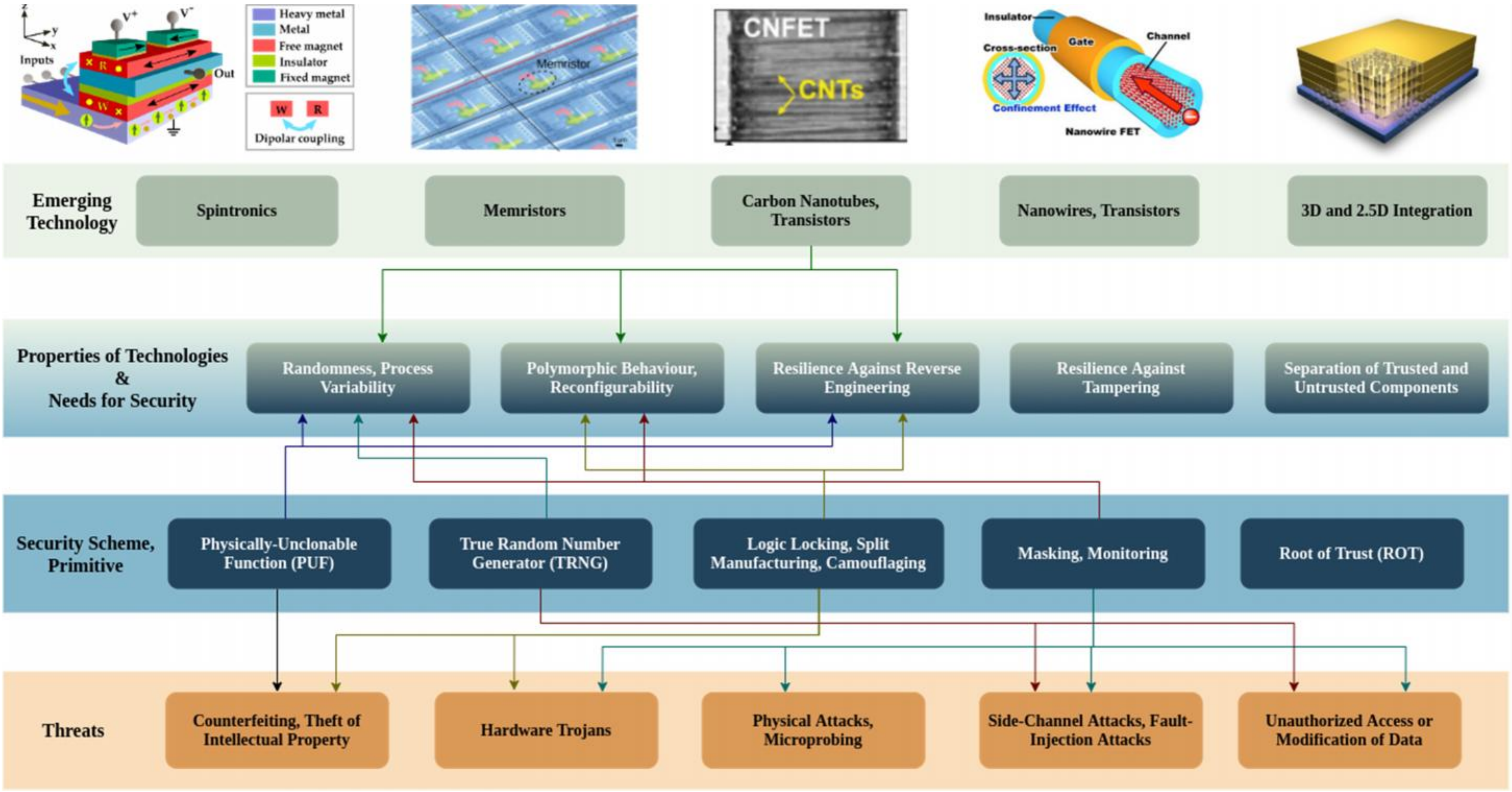
Wu et al., JSSC 2018

Basics of Carbon Nanotube Transistors



Shulaker et al., Nature 2013

Carbon Nanotubes for Hardware Security



Emerging Technology

Spintronics

Memristors

Carbon Nanotubes, Transistors

Nanowires, Transistors

3D and 2.5D Integration

Properties of Technologies & Needs for Security

Randomness, Process Variability

Polymorphic Behaviour, Reconfigurability

Resilience Against Reverse Engineering

Resilience Against Tampering

Separation of Trusted and Untrusted Components

Security Scheme, Primitive

Physically-Unclonable Function (PUF)

True Random Number Generator (TRNG)

Logic Locking, Split Manufacturing, Camouflaging

Masking, Monitoring

Root of Trust (ROT)

Threats

Counterfeiting, Theft of Intellectual Property

Hardware Trojans

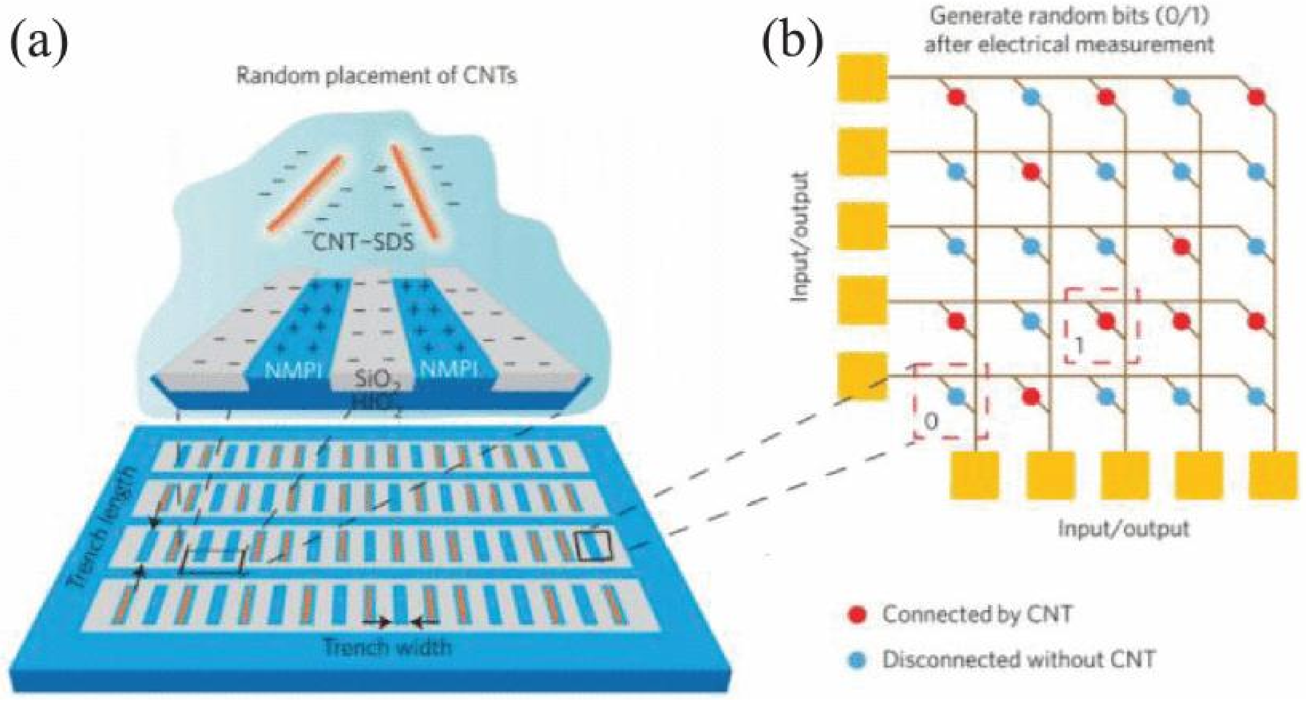
Physical Attacks, Microprobing

Side-Channel Attacks, Fault-Injection Attacks

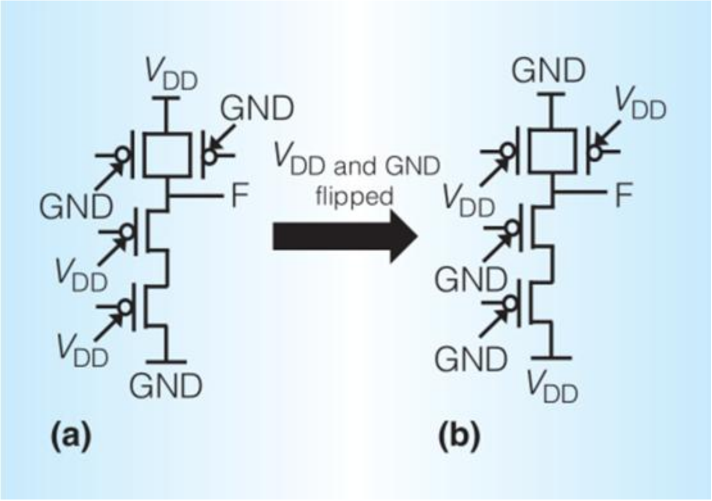
Unauthorized Access or Modification of Data

Carbon Nanotubes for Hardware Security

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



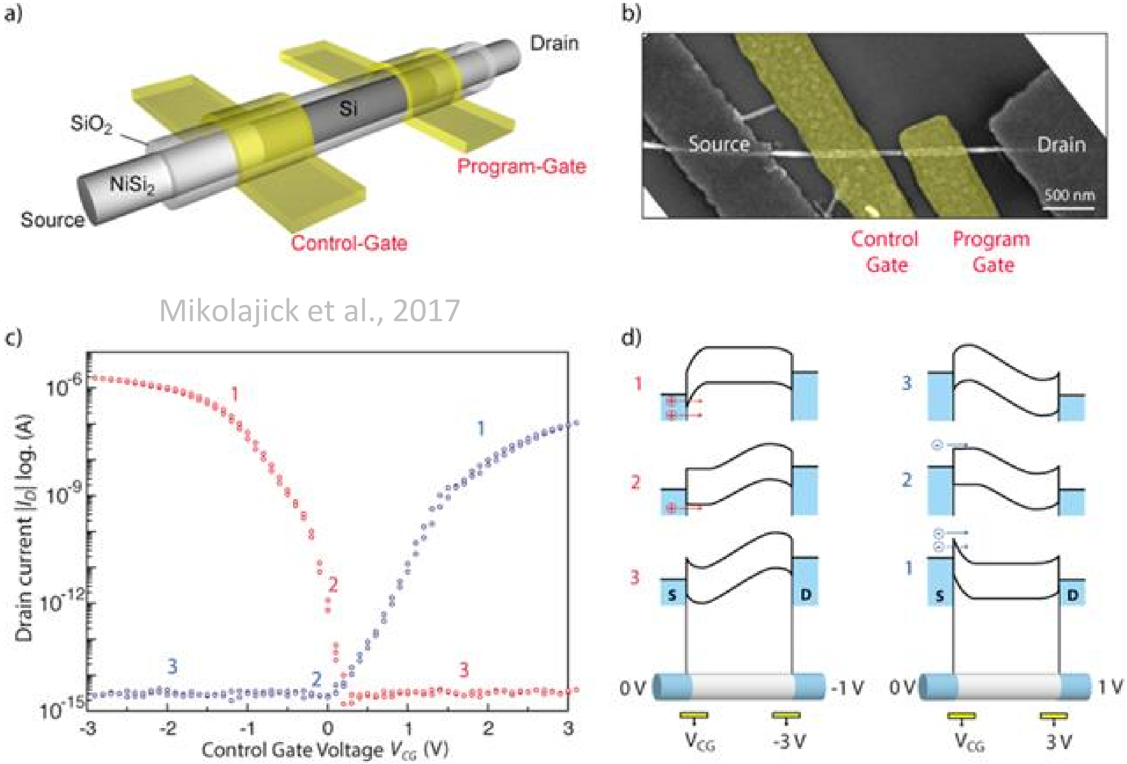
Rahman et al., TVLSI, 2017



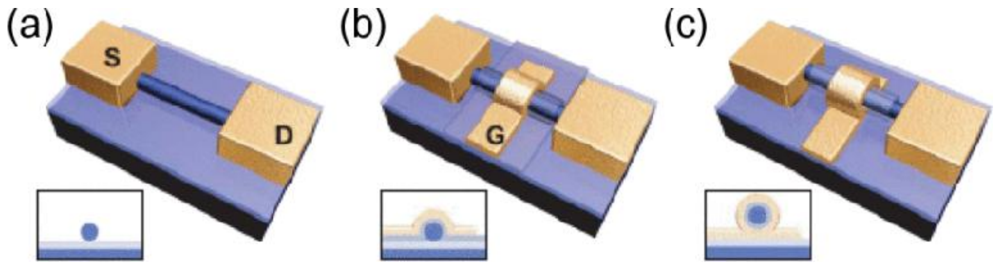
Suresh et al., Micro, 2016

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

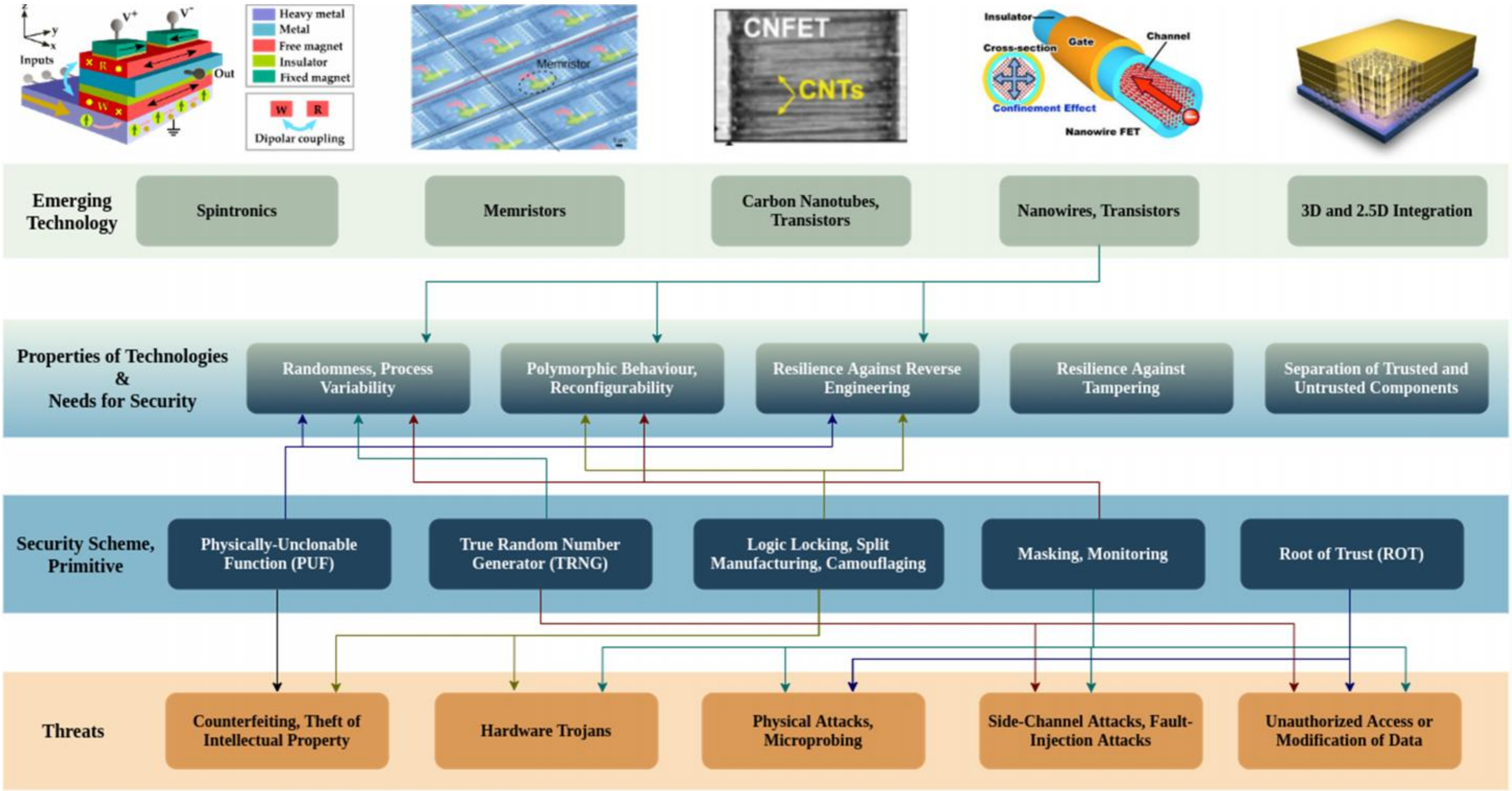


Mikolajick et al., 2017



Lu et al., TED 2008

Nanowire Transistors for Hardware Security



Emerging Technology: Spintronics; Memristors; Carbon Nanotubes, Transistors; Nanowires, Transistors; 3D and 2.5D Integration

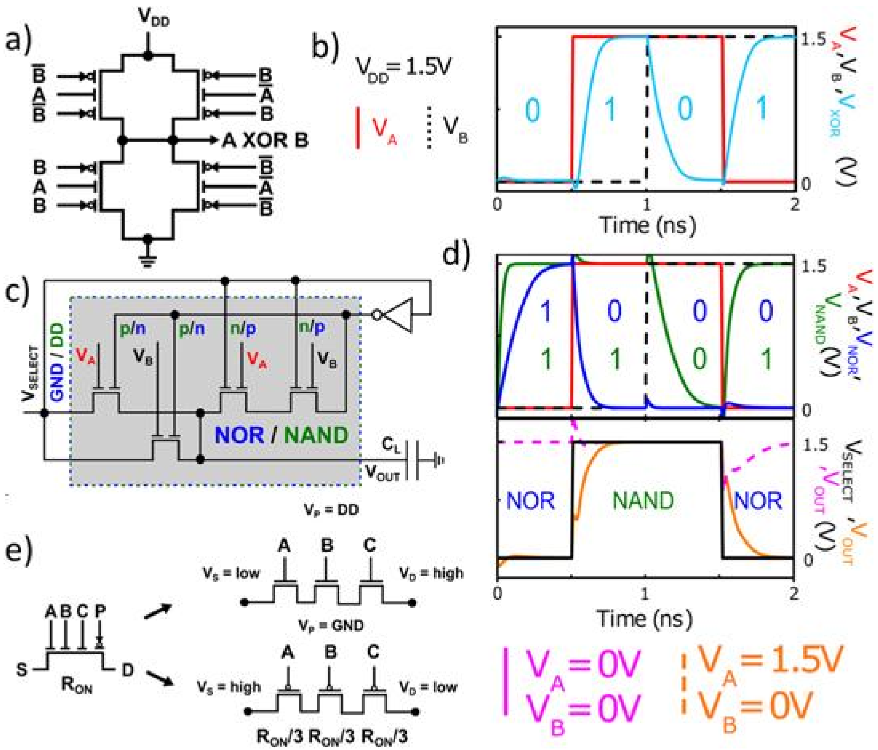
Properties of Technologies & Needs for Security: Randomness, Process Variability; Polymorphic Behaviour, Reconfigurability; Resilience Against Reverse Engineering; Resilience Against Tampering; Separation of Trusted and Untrusted Components

Security Scheme, Primitive: Physically-Unclonable Function (PUF); True Random Number Generator (TRNG); Logic Locking, Split Manufacturing, Camouflaging; Masking, Monitoring; Root of Trust (ROT)

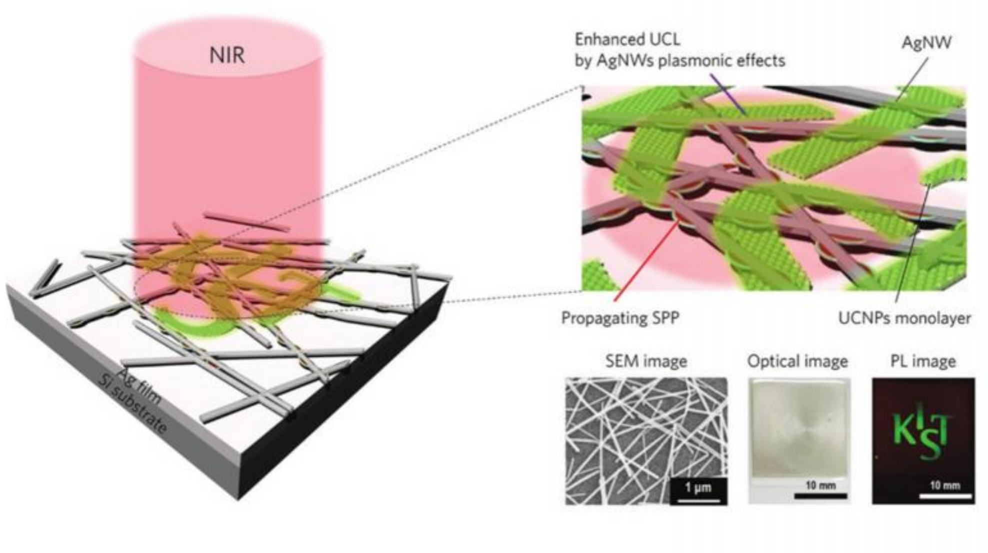
Threats: Counterfeiting, Theft of Intellectual Property; Hardware Trojans; Physical Attacks, Microprobing; Side-Channel Attacks, Fault-Injection Attacks; Unauthorized Access or Modification of Data

Nanowire Transistors for Hardware Security

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



Mikolajick et al., 2017

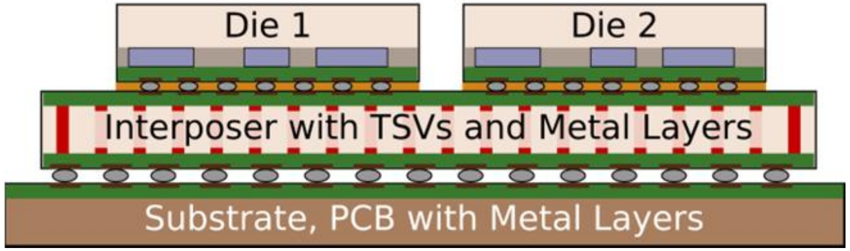


Park et al., 2016

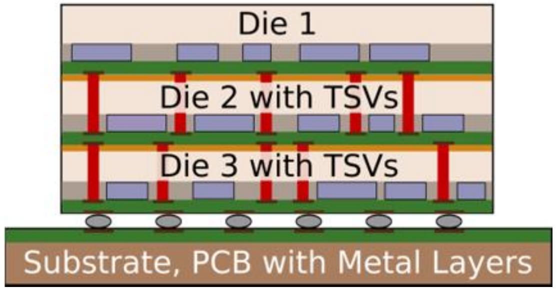
Basics of 3D and 2.5D Integration

- Shorter, vertical interconnects: power consumption, delay, bandwidth – “More Moore”
- Separate dies: heterogeneous and larger systems, yield – “More than Moore”

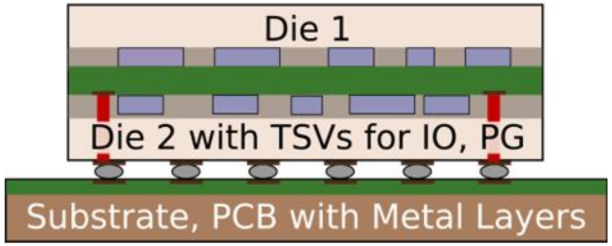
Interposer Stack


Die 1
Die 2
Interposer with TSVs and Metal Layers
Substrate, PCB with Metal Layers

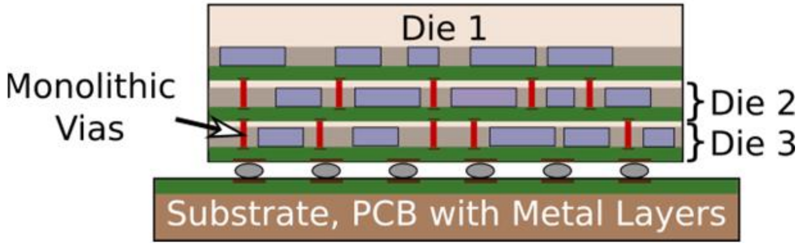
TSV-based 3D IC



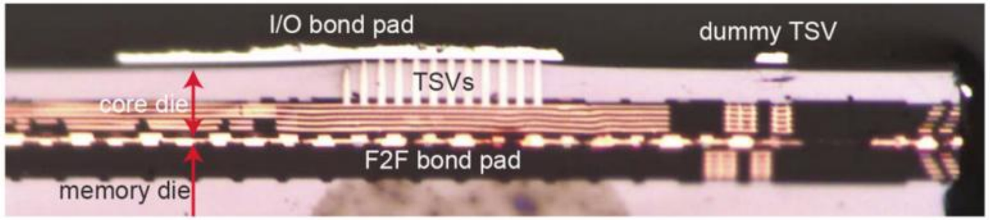
F2F 3D IC



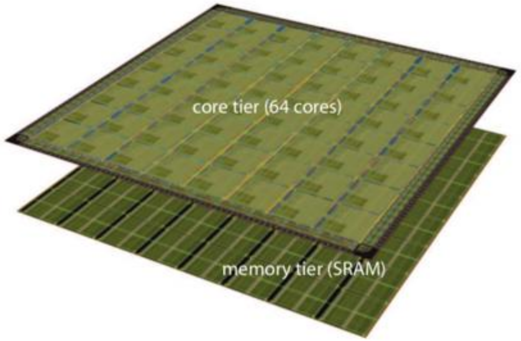
Monolithic 3D IC

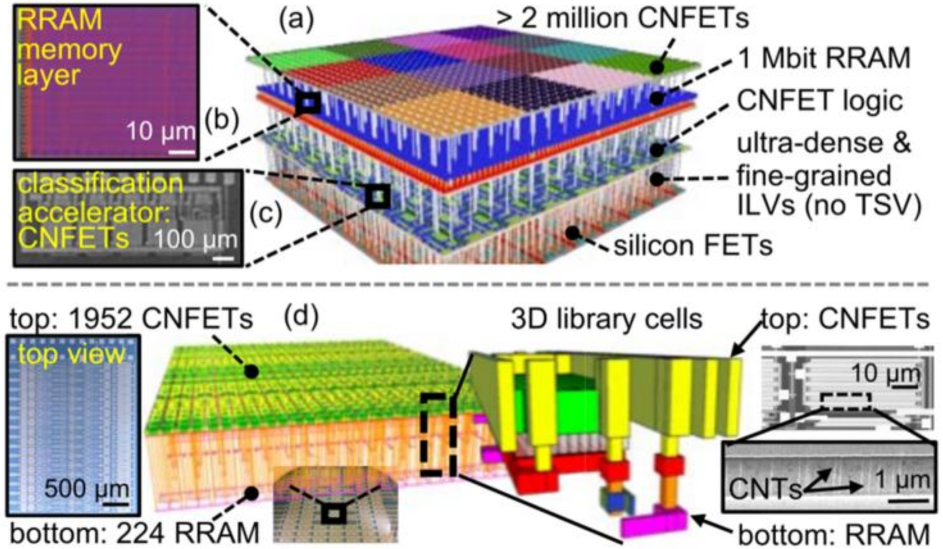


Basics of 3D and 2.5D Integration

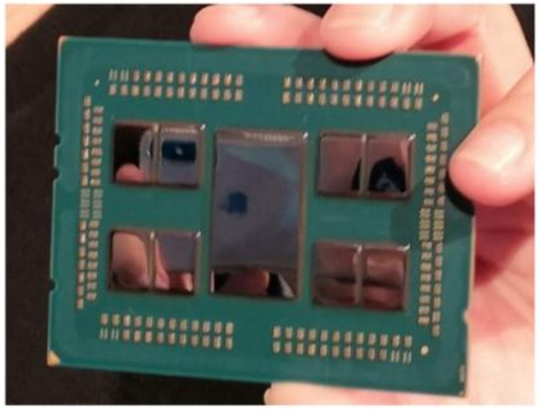


Kim et al., ISSCC, 2012

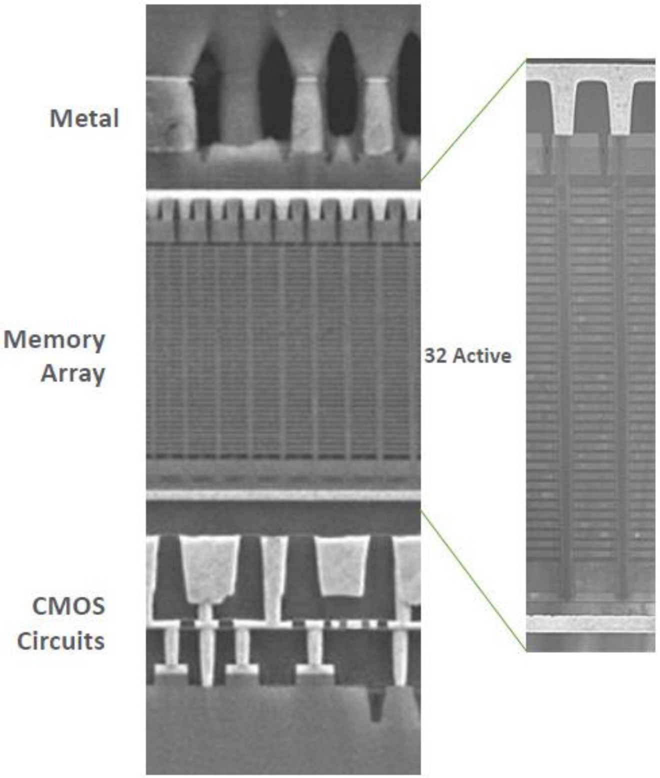




Aly et al., Proc. IEEE, 2019

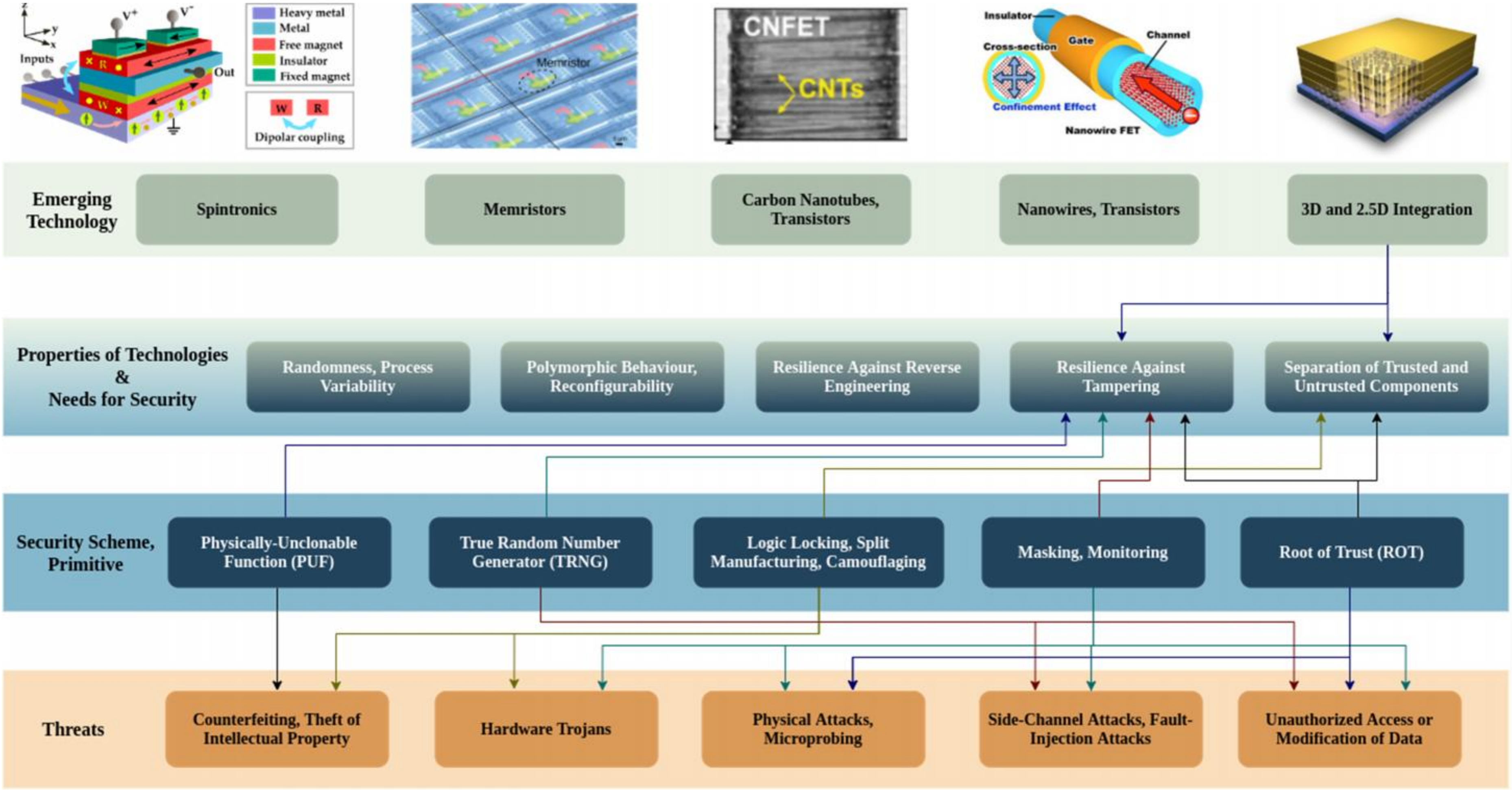


3D NAND Structure



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

3D and 2.5D Integration for Hardware Security



Emerging Technology: Spintronics; Memristors; Carbon Nanotubes, Transistors; Nanowires, Transistors; 3D and 2.5D Integration

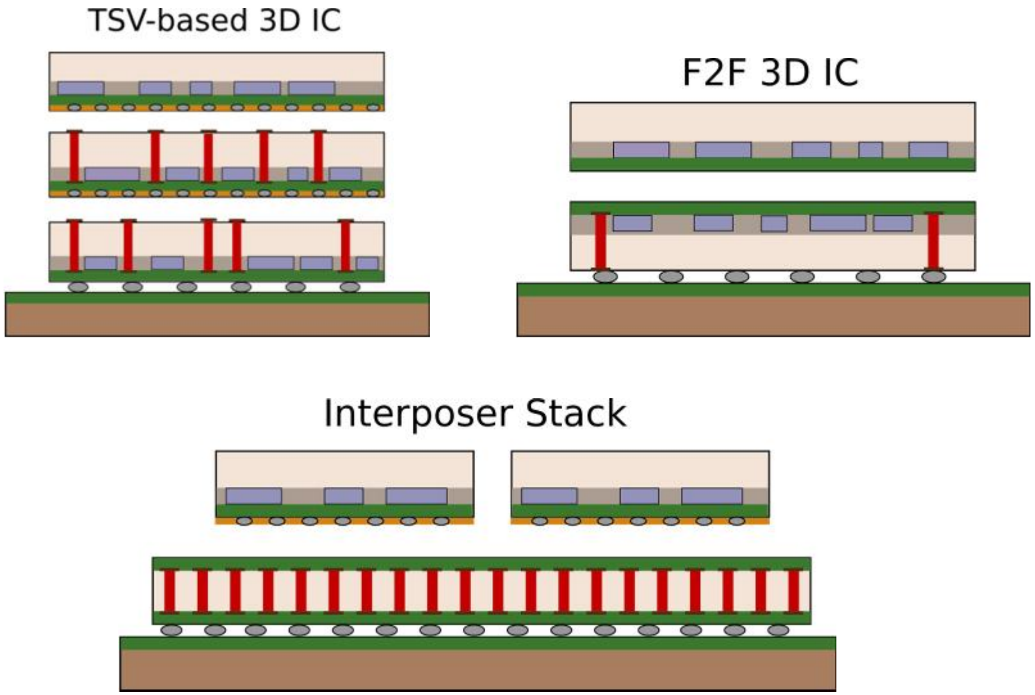
Properties of Technologies & Needs for Security: Randomness, Process Variability; Polymorphic Behaviour, Reconfigurability; Resilience Against Reverse Engineering; Resilience Against Tampering; Separation of Trusted and Untrusted Components

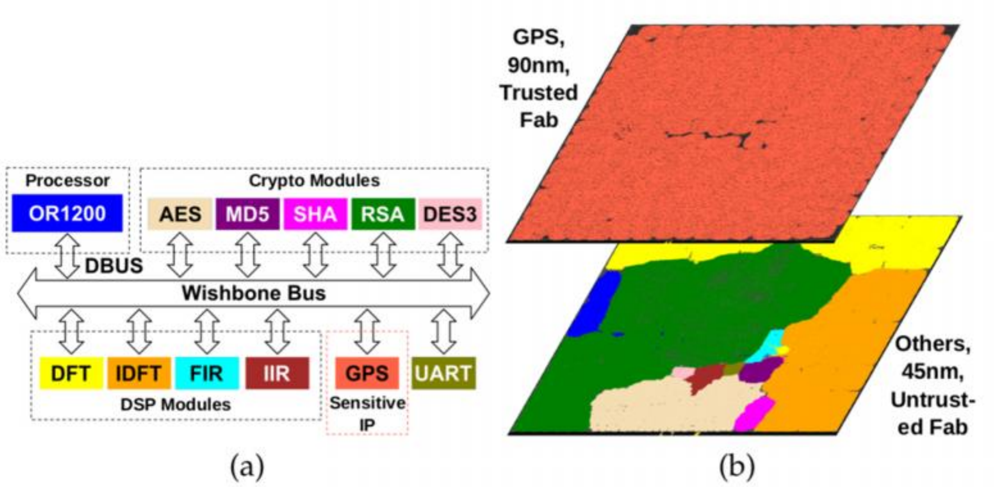
Security Scheme, Primitive: Physically-Unclonable Function (PUF); True Random Number Generator (TRNG); Logic Locking, Split Manufacturing, Camouflaging; Masking, Monitoring; Root of Trust (ROT)

Threats: Counterfeiting, Theft of Intellectual Property; Hardware Trojans; Physical Attacks, Microprobing; Side-Channel Attacks, Fault-Injection Attacks; Unauthorized Access or Modification of Data

3D and 2.5D for Split Manufacturing

- 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)

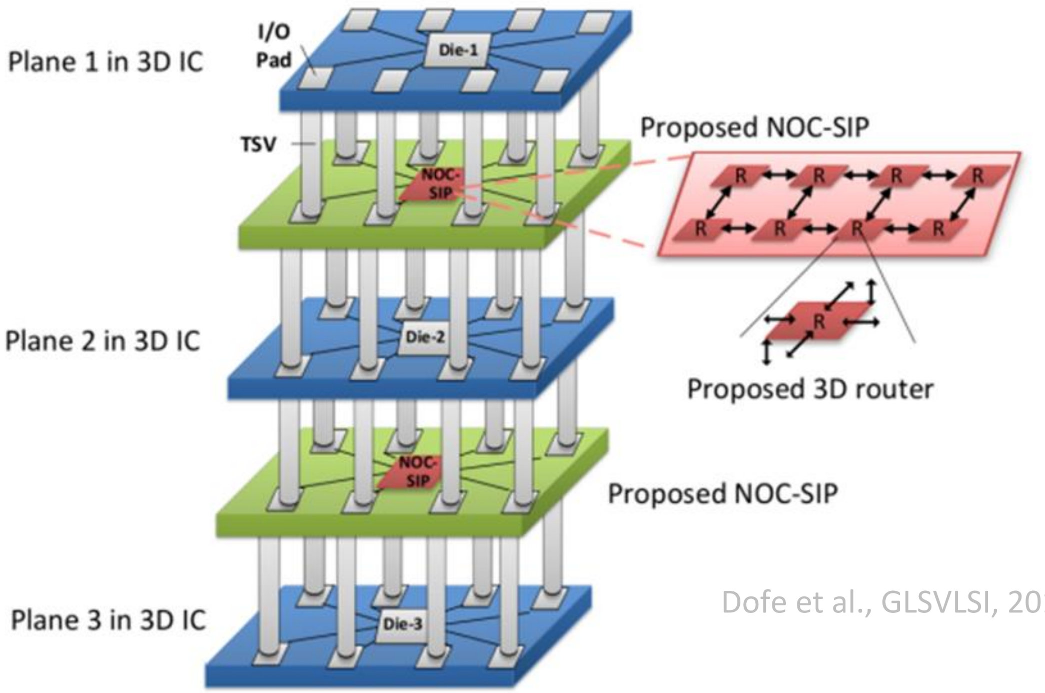




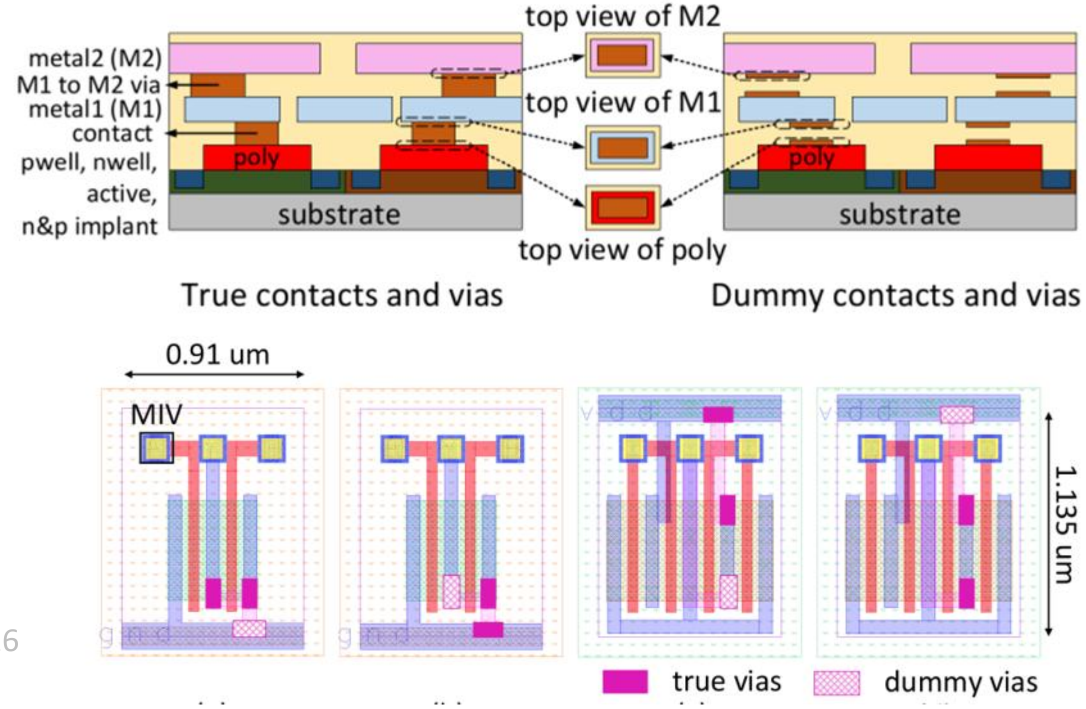
Patnaik et al., TETC, 2019

3D and 2.5D for Split Manufacturing, Camouflaging

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



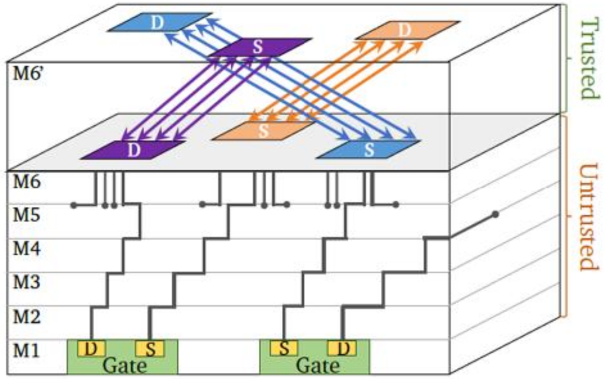
Dofe et al., GLSVLSI, 2016

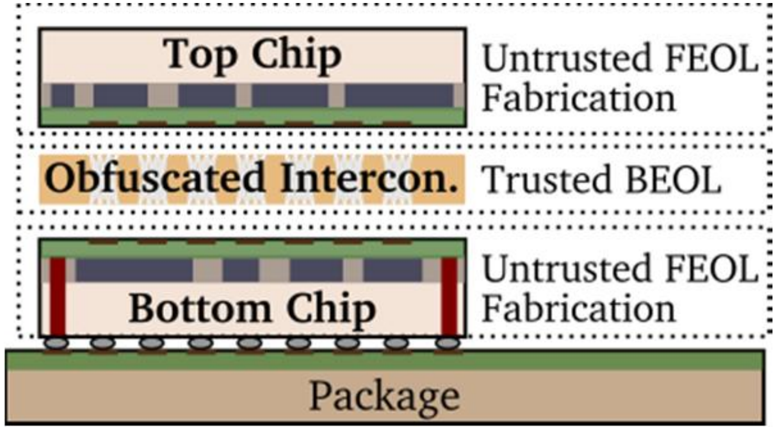


Yan et al., TCS, 2018

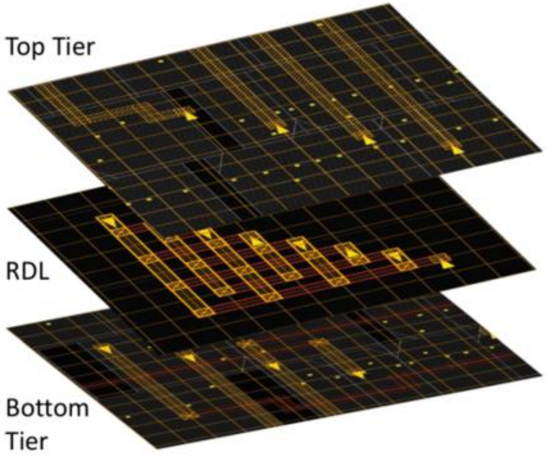
3D and 2.5D for Split Manufacturing & Camouflaging

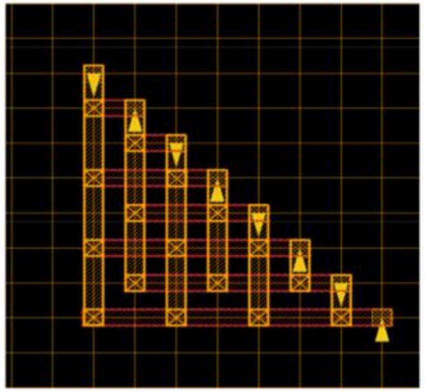
- Only trusted BEOL and resilient BEOL materials required
- Thwarts both malicious foundries and end-user
- Reasonable layout cost





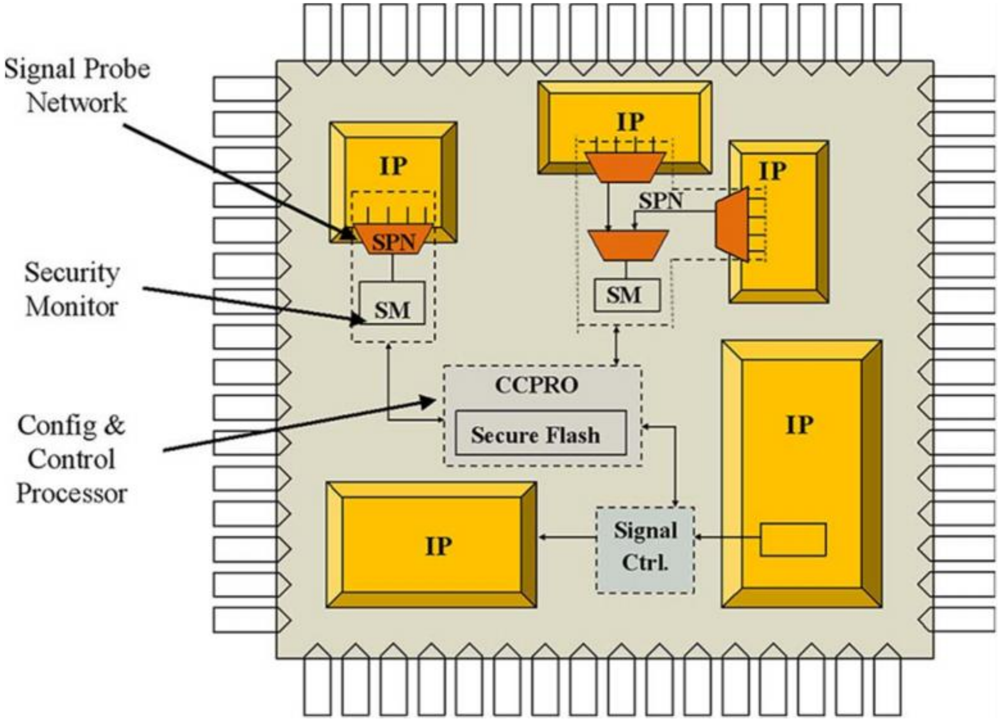
Patnaik et al., ICCAD, 2018



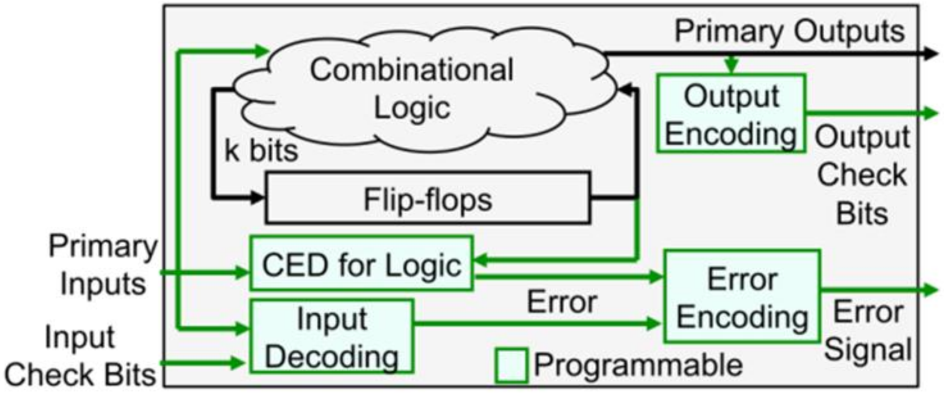


Obfuscated switchbox in RDL

3D and 2.5D for Runtime Security: Monitoring



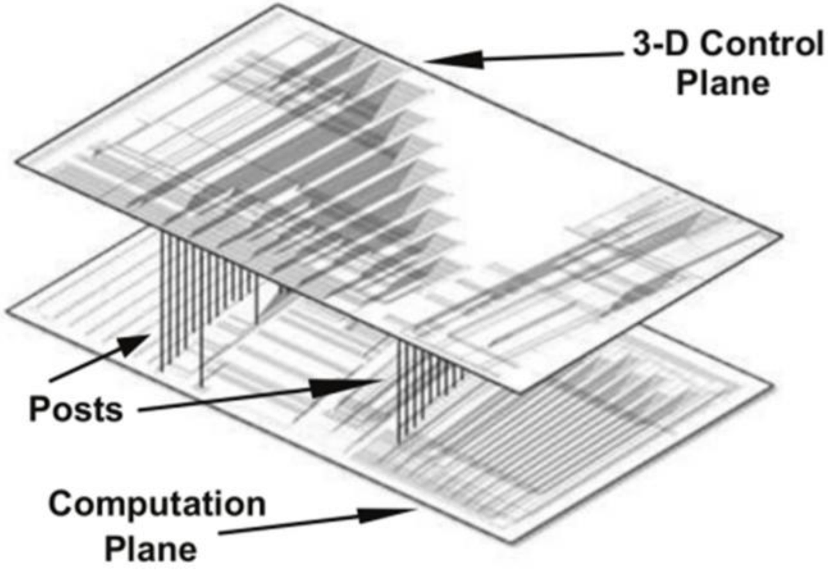
Bhunia et al., Proc. IEEE, 2014



Wu et al., TCAD 2016

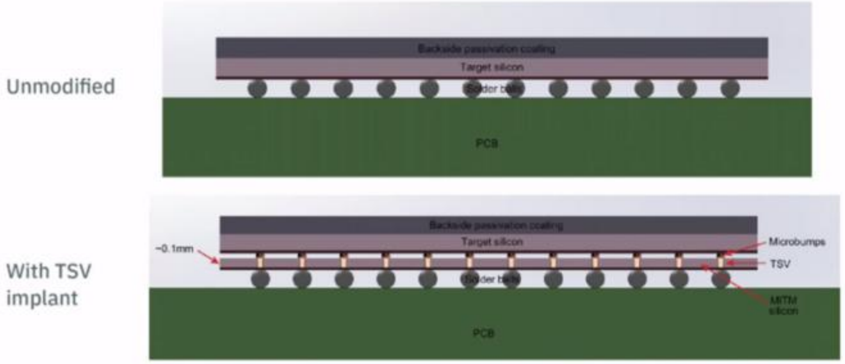
3D and 2.5D for Runtime Security: Monitoring

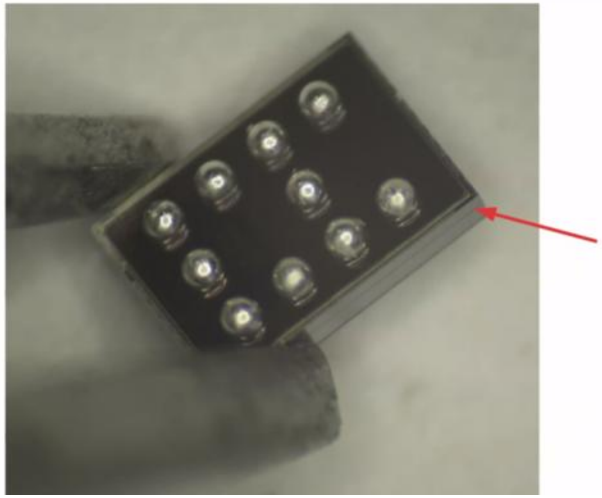
- Physical separation
- Still, beware 3rd parties involved for integration



Valamehr et al., ACSAC, 2010

TSV + WLCSP = Nearly Undetectable Implant





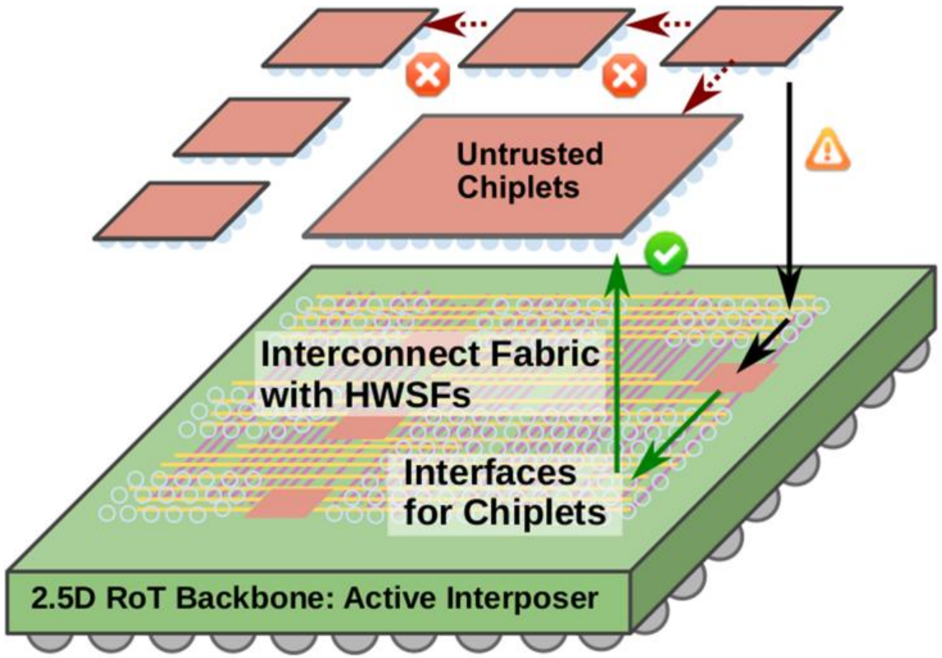
Detection?

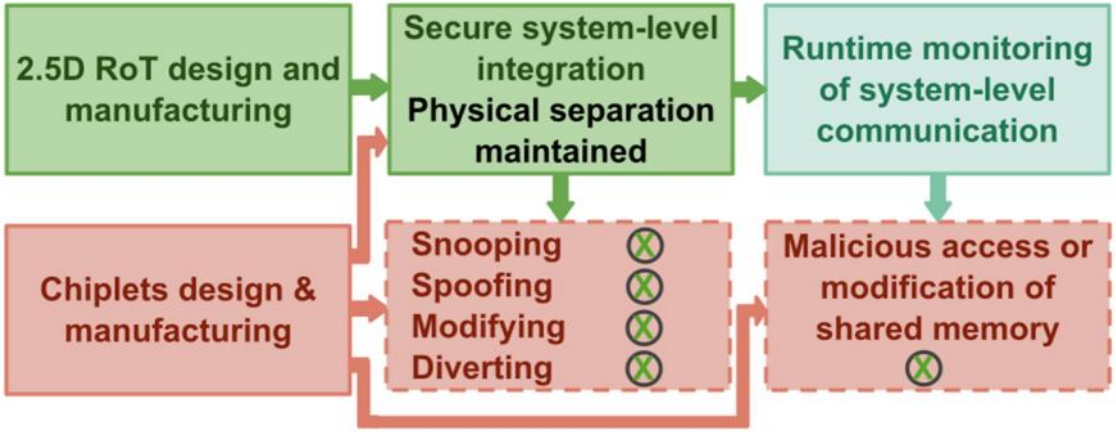
- Many WLCSP already have a small seam
- A well-done WLCSP implant will have almost no X-ray footprint

"bunnie" Huang, 36C3, 2019

3D and 2.5D for Runtime Security: Monitoring

- Physical separation and dedicated hardware for root of trust

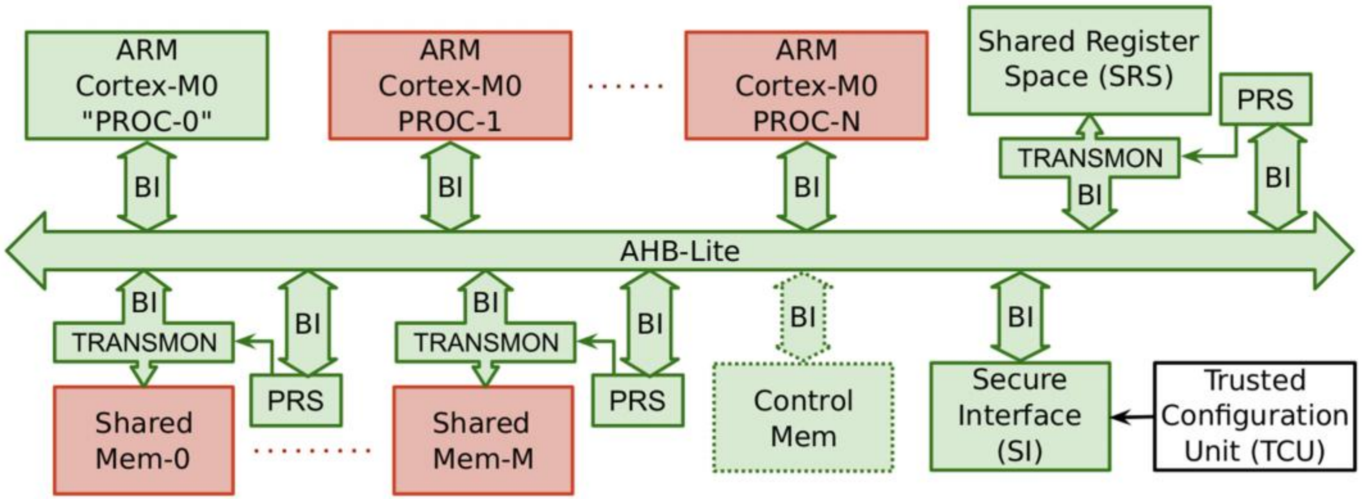


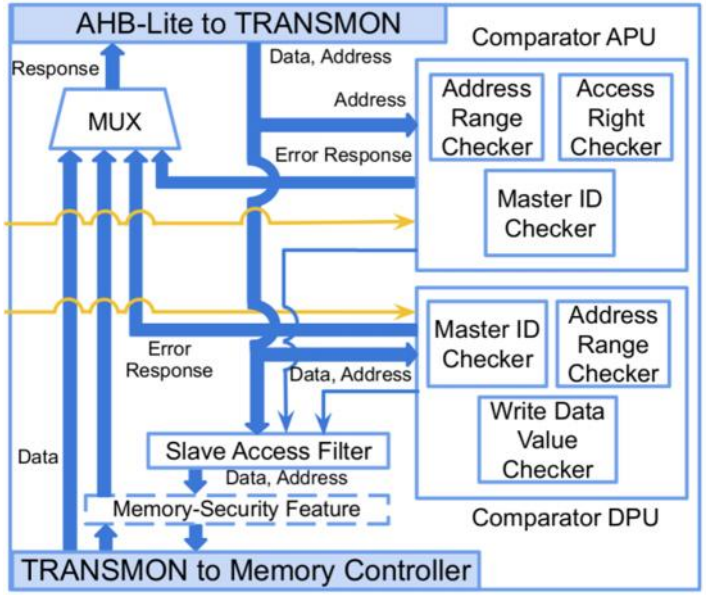

2.5D RoT design and manufacturing
Secure system-level integration
Physical separation maintained
Runtime monitoring of system-level communication
Chiplets design & manufacturing
Snooping ⓧ
Spoofing ⓧ
Modifying ⓧ
Diverting ⓧ
Malicious access or modification of shared memory
ⓧ

Nabeel et al., TC, 2020

3D and 2.5D for Runtime Security: Monitoring

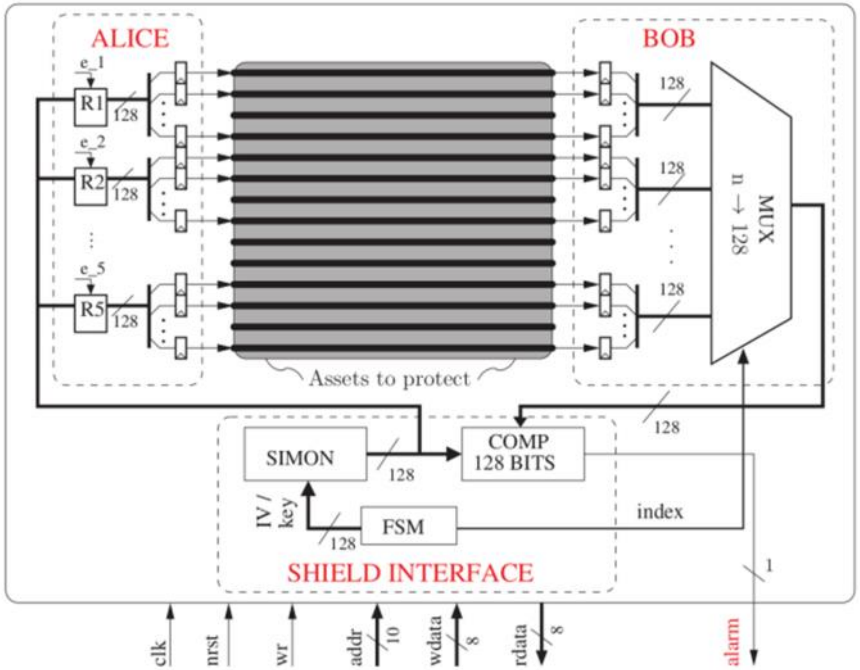
- Physical separation and dedicated hardware for root of trust



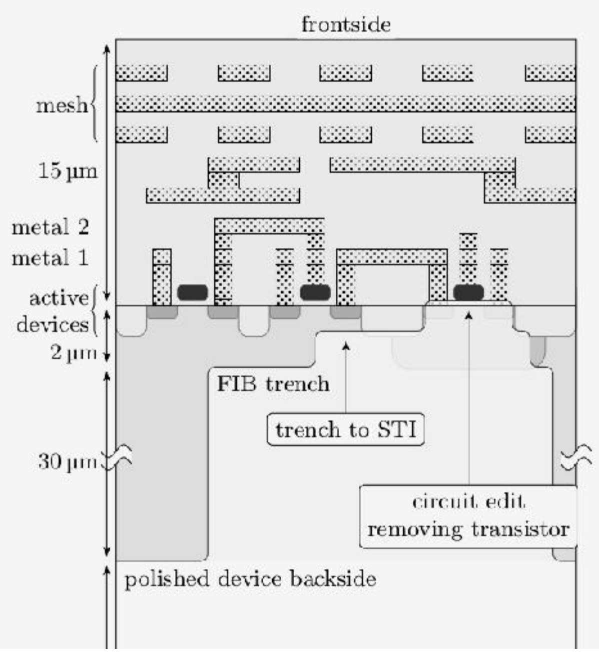


Nabeel et al., TC, 2020

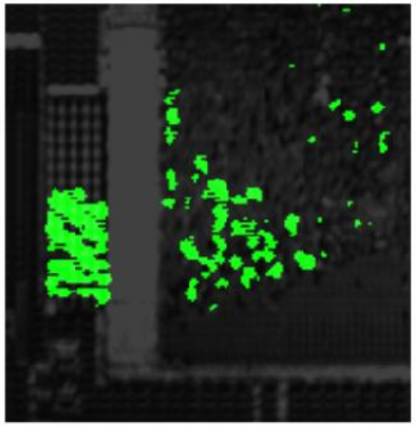
3D and 2.5D for Runtime Security: Physical Protection



Ngo et al., TC, 2017



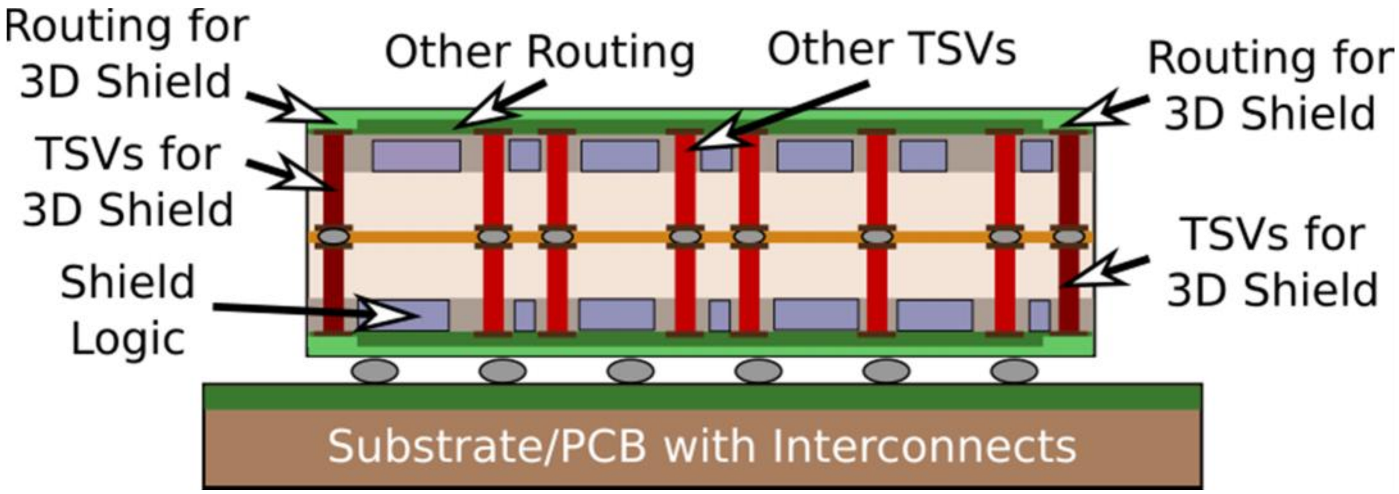
Helfmeier et al., CCS, 2013



Tajik et al., CCS, 2017

3D and 2.5D for Runtime Security: Physical Protection

- Physical enclosure, “cage all around”
- Could also block side-channel emissions and hinder fault injection

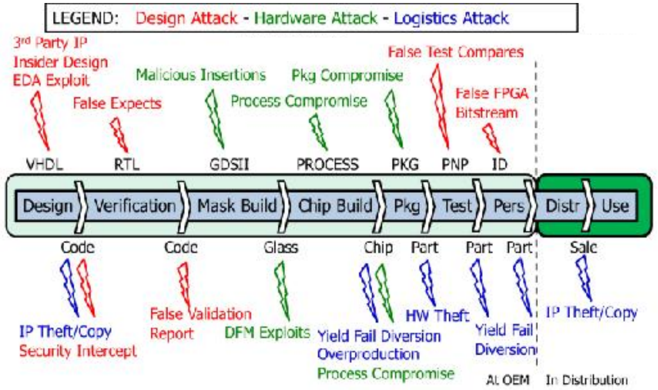


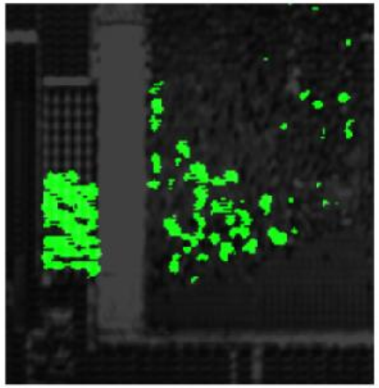
Knechtel et al., IOLTS, 2019

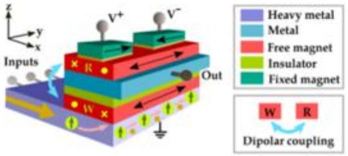
Notes on Challenges for Beyond-CMOS Hardware Security

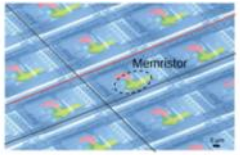
- Establish closer links between communities
- Joint (re-)definition of security metrics
  - „Translation“ especially for technology-specific aspects, e.g., PUFs
- Joint reconsideration of threat models
- Technology exploration hand in hand with development of security schemes
- Most technologies are CMOS compatible/hybrid – identification of “weakest link in chain”

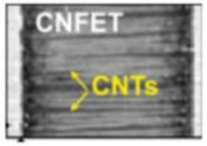
Hardware Security for and beyond CMOS Technology

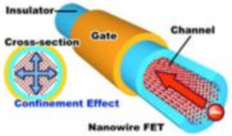


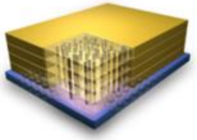


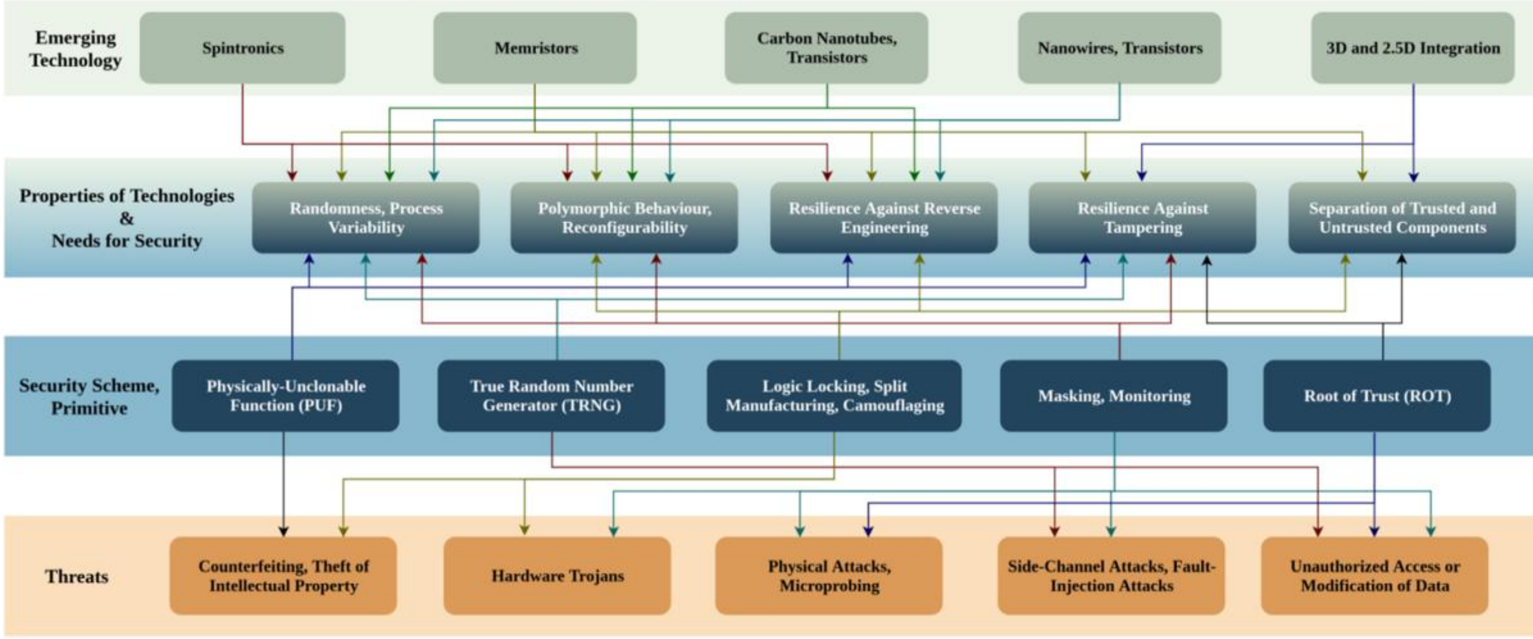












Emerging Technology

Spintronics

Memristors

Carbon Nanotubes, Transistors

Nanowires, Transistors

3D and 2.5D Integration

Properties of Technologies & Needs for Security

Randomness, Process Variability

Polymorphic Behaviour, Reconfigurability

Resilience Against Reverse Engineering

Resilience Against Tampering

Separation of Trusted and Untrusted Components

Security Scheme, Primitive

Physically-Unclonable Function (PUF)

True Random Number Generator (TRNG)

Logic Locking, Split Manufacturing, Camouflaging

Masking, Monitoring

Root of Trust (ROT)

Threats

Counterfeiting, Theft of Intellectual Property

Hardware Trojans

Physical Attacks, Microprobing

Side-Channel Attacks, Fault-Injection Attacks

Unauthorized Access or Modification of Data

wp.nyu.edu/johann arxiv.org/abs/2001.08780

Thank you!