CPEG 422/622 EMBEDDED SYSTEMS DESIGN

MW 3:35 – 4:50, SHARP 116

Chengmo Yang

chengmo@udel.edu

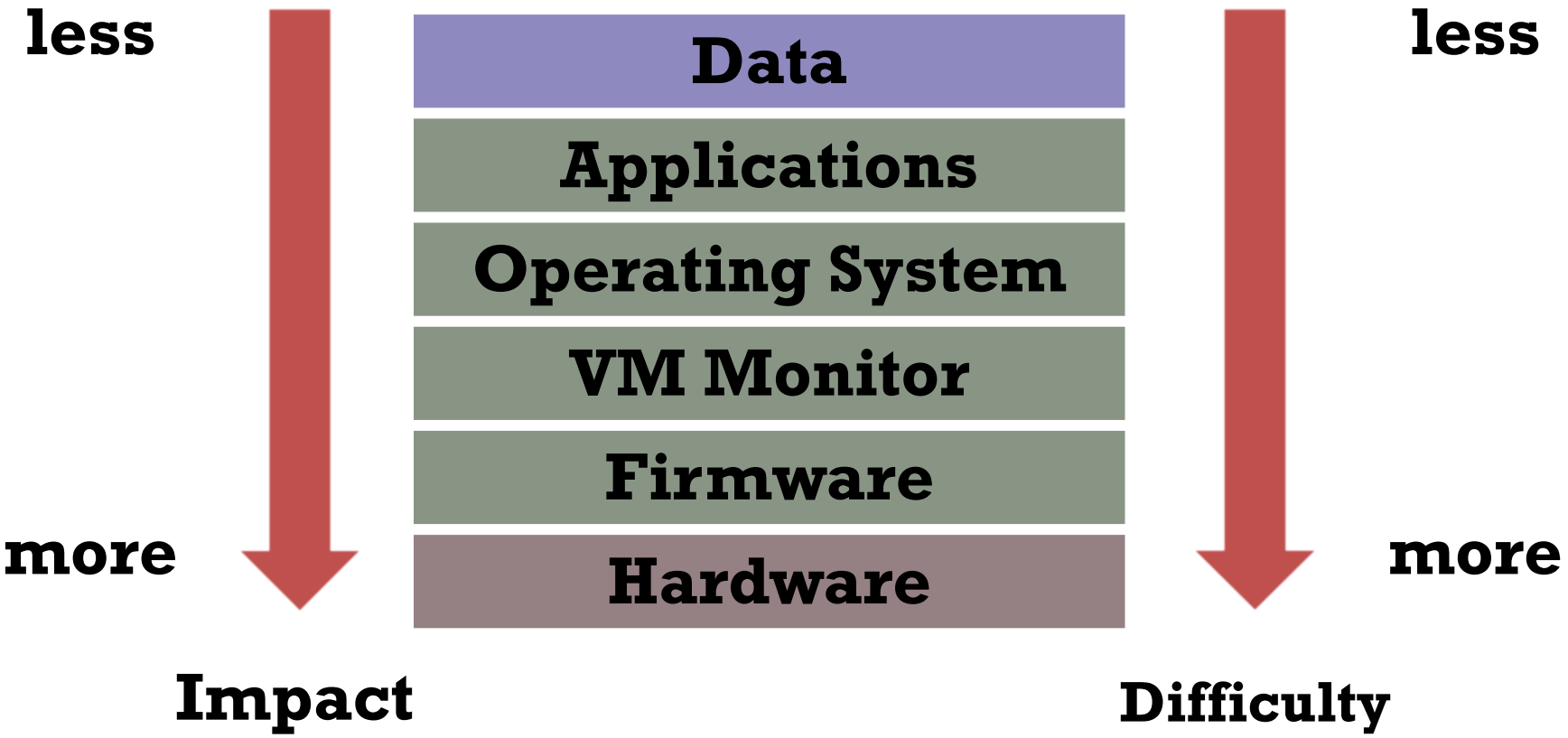
Evans 201C

LECTURE 15
HW SECURITY

OUTLINE

- What is hardware security?
- Threats and Countermeasures
  - Hardware Trojan
  - Reverse Engineering

ATTACK IMPACT AND DIFFICULTY

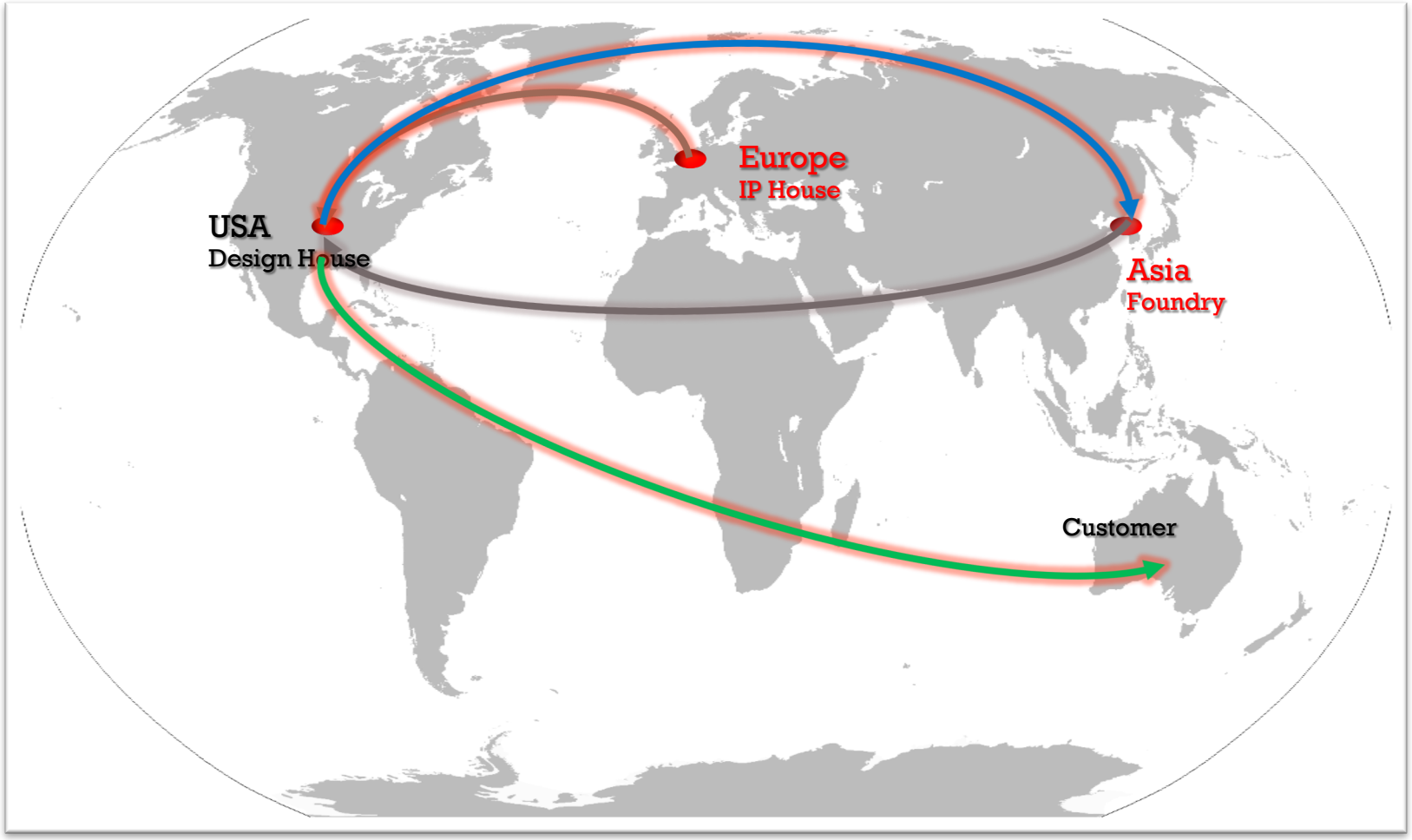


HW used to be the trust anchor,
But not any more

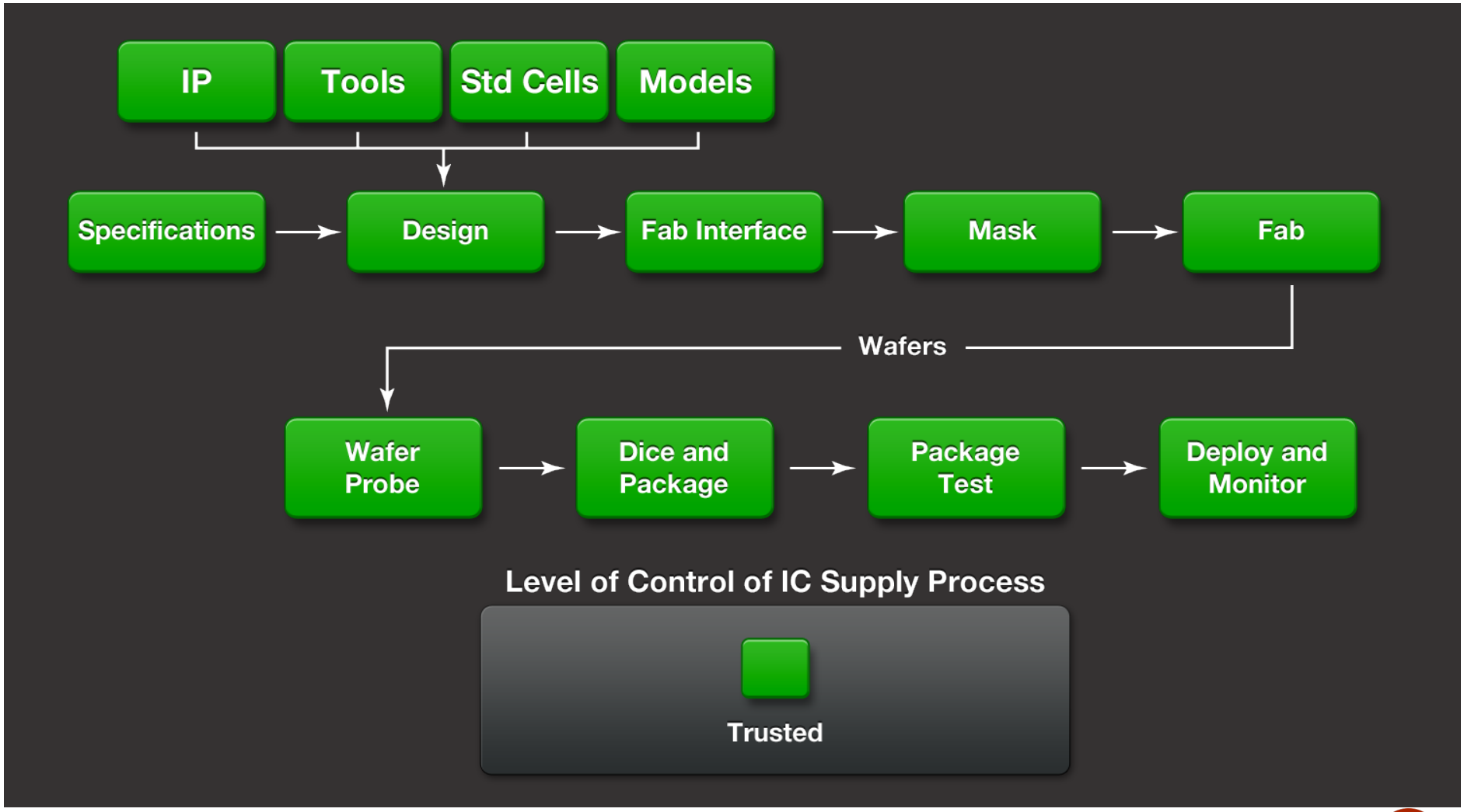
HARDWARE SECURITY

- Security of electronic hardware
  - Architecture, Implementation, Validation
  - Focus on attacks & mitigations
- Assets: the HW components themselves
- Threats:
  - Side channel attacks
  - Fault injection attacks, probing attacks
  - Cryptographic Hardware attacks
  - Debug interface attacks, untrusted CAD
  - Supply chain attacks
    - Hardware Trojans Horses, PCB tampering
    - Overproduction, IP theft, reverse engineering
    - Counterfeiting, remarking, recycling

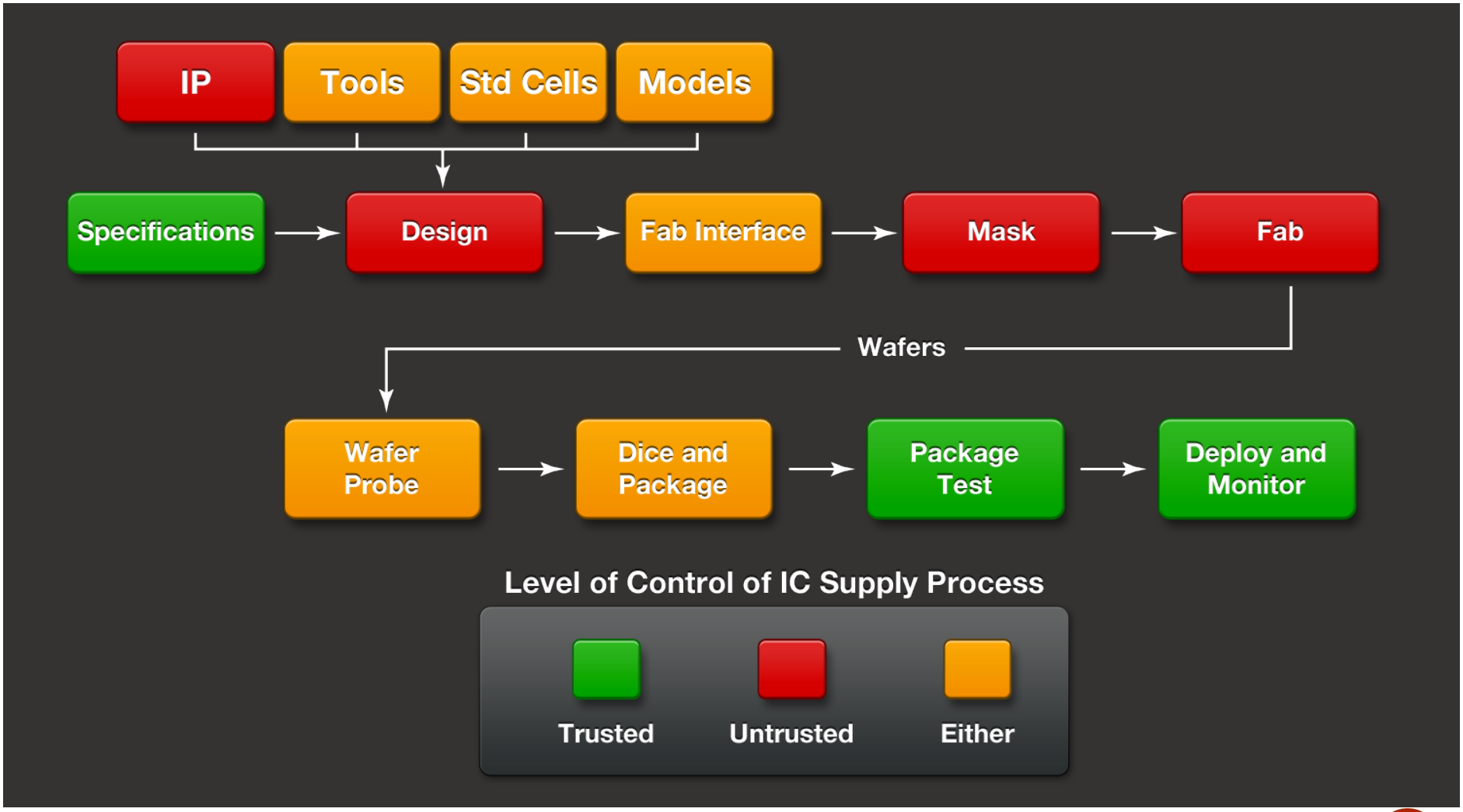
GLOBALIZED SUPPLY CHAIN



EVOLUTION OF THE SUPPLY CHAIN (PAST)



Evolution of the Supply Chain (Now)

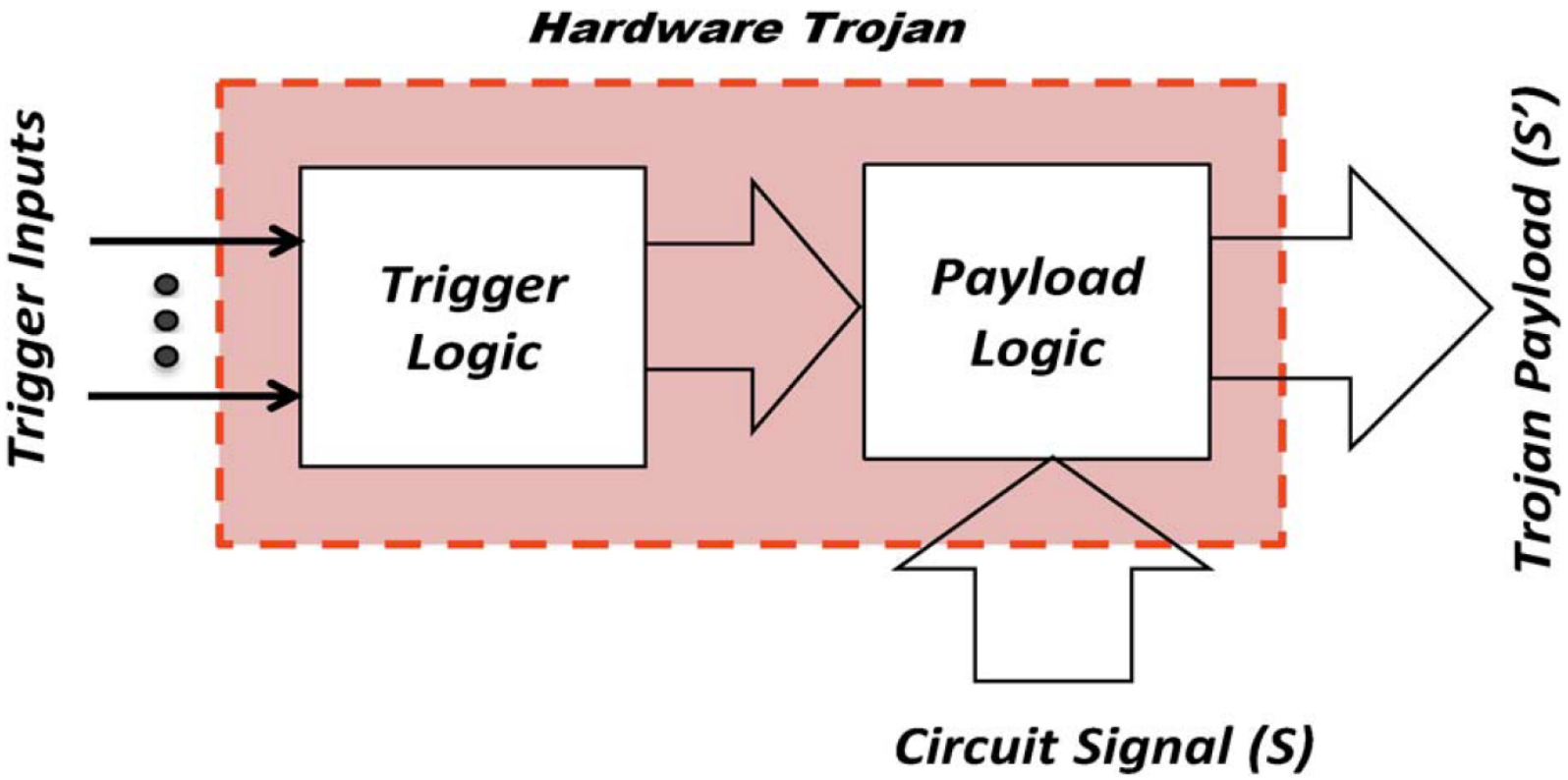


HARDWARE TROJANS

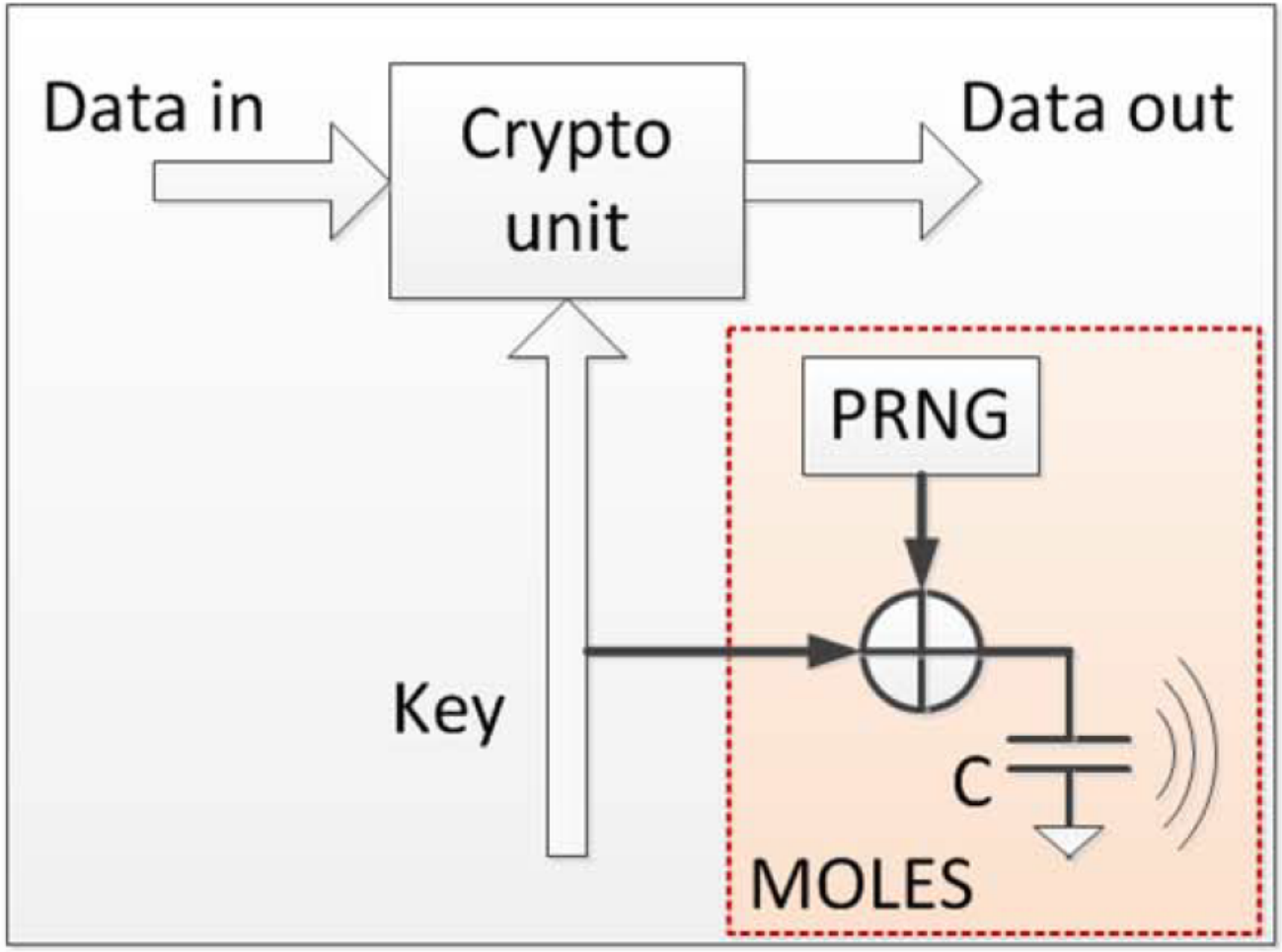
- Malicious, stealthy modifications of the original hardware design
  - E.g., changes in the circuit, state machine

- Attacker Goals:
  - Exploit hardware
  - Use hardware to create backdoors
  - Leak sensitive or private information
    - E.g., keys
  - DoS attacks or performance degradation
    - E.g., disable branch prediction
  - Reliability attacks, aging

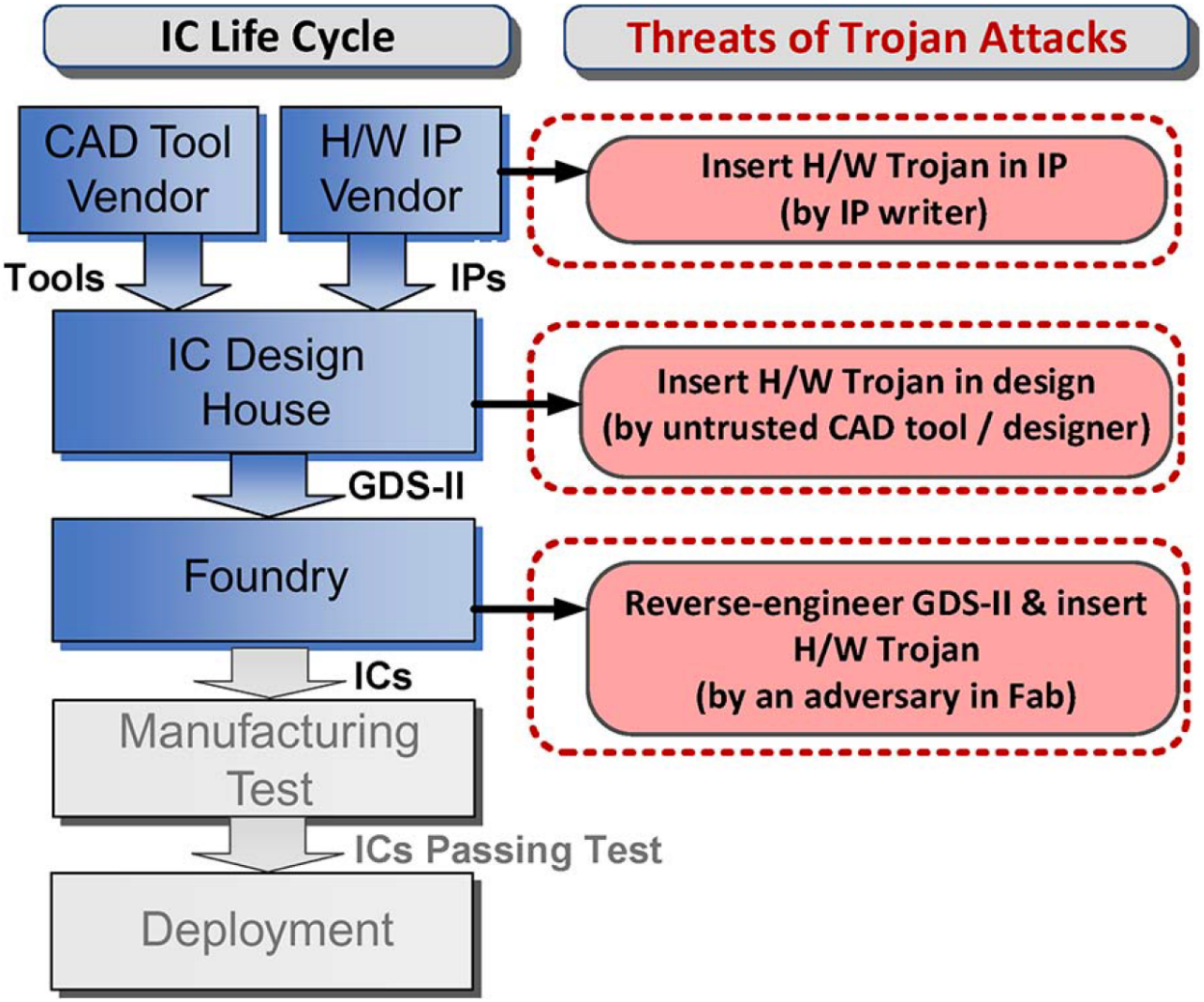
BASIC HARDWARE TROJAN DESIGN



LEAKAGE TROJAN EXAMPLE

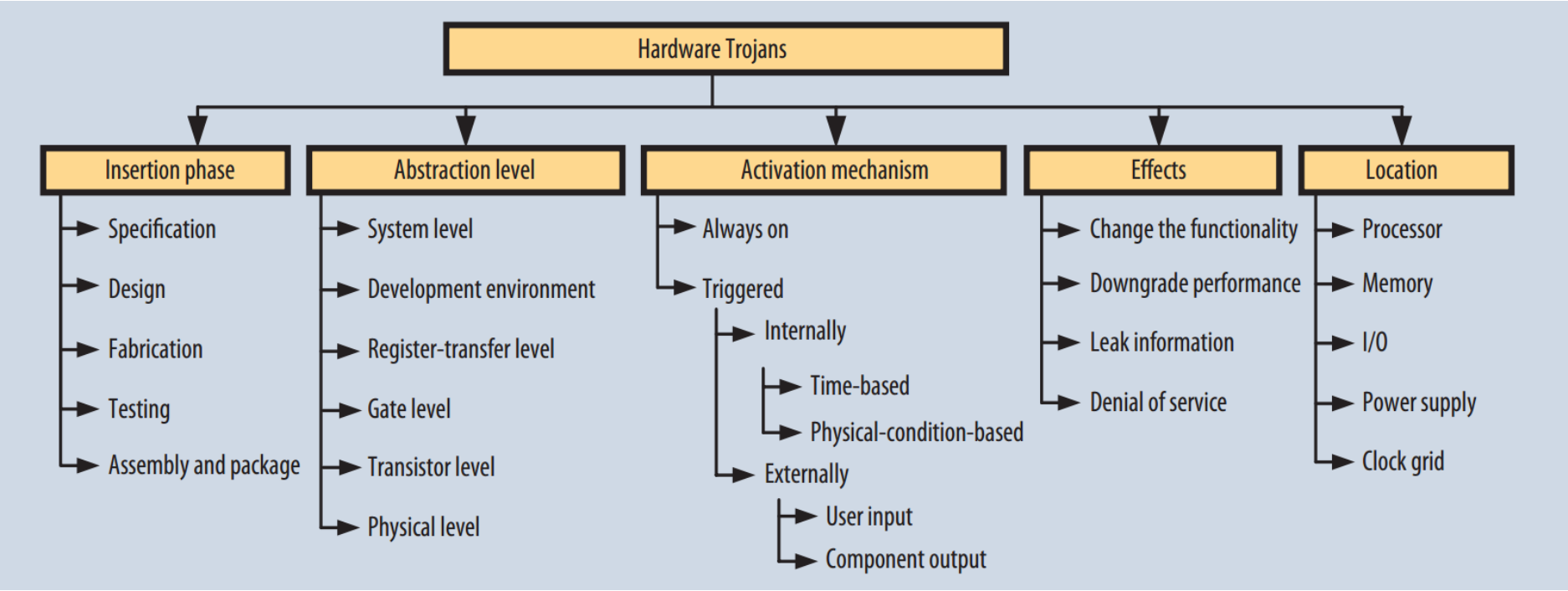


TROJAN INSERTION STAGES



Bhunia *et al.* "Hardware Trojan Attacks: Threat Analysis and Countermeasures," Proc. of IEEE, 2014

HARDWARE TROJAN TAXONOMY



More details can be found at:
https://www.trust-hub.org/resource/pdf/Taxonomy.pdf

HARDWARE TROJANS VS FAULTS

	Fault	Hardware Trojan
Activation	Usually at known functional state	Arbitrary combination/sequence of internal circuit states (digital/analog)
Insertion Agent	*Accidental* (due to imperfection in manufacturing process)	*Intentional* (inserted by an adversary during IC design or fabrication)
Manifestation	Functional/parametric failure	Functional/parametric failure or information leakage

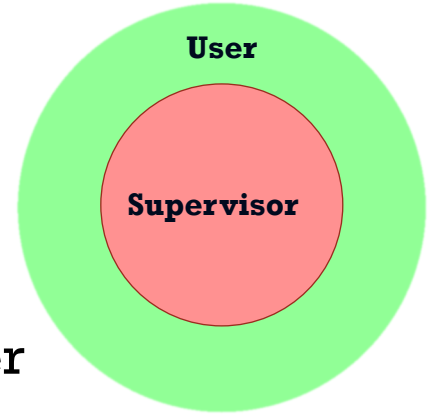
HARDWARE VS SOFTWARE TROJANS

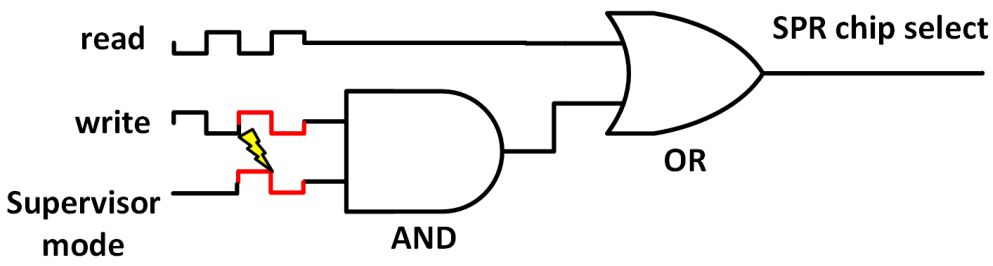
	Software Trojan	Hardware Trojan
Activation	A type of malware that resides in a code and activates during its execution	Resides in hardware (e.g. IC) and activates during its operation
Infection	Spreads through user interaction e.g. downloading and running a file from Internet	Inserted through untrusted entities in design or fabrication house
Remedy	Can be *removed in field* through S/W support	*Cannot be removed* once IC is fabricated

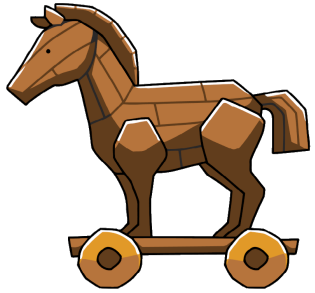
Bhunia *et al.* "Hardware Trojan Attacks: Threat Analysis and Countermeasures," Proc. of IEEE, 2014

CONCRETE HARDWARE TROJAN EXAMPLE

- Processors have privilege "rings" to enable memory access control
  - The OpenRISC processor has only 2 levels: User, Supervisor
- It is possible to inject a Trojan with a hidden trigger
  - The hardware circuit of the CPU uses a supervisor signal to enable access

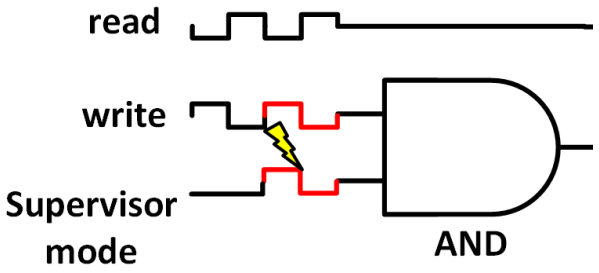


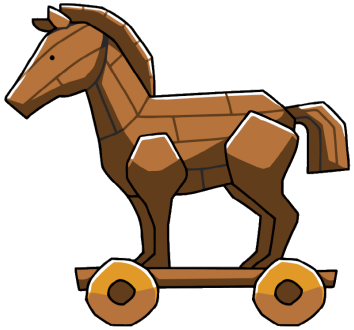


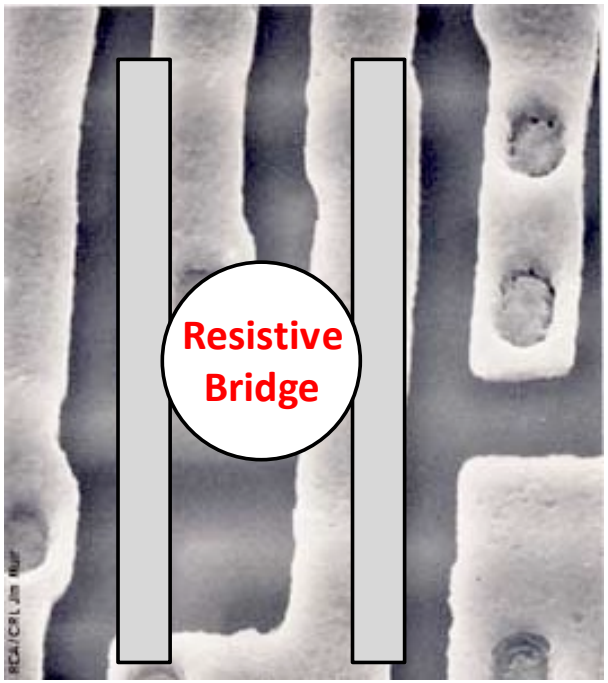


CONCRETE HARDWARE TROJAN EXAMPLE

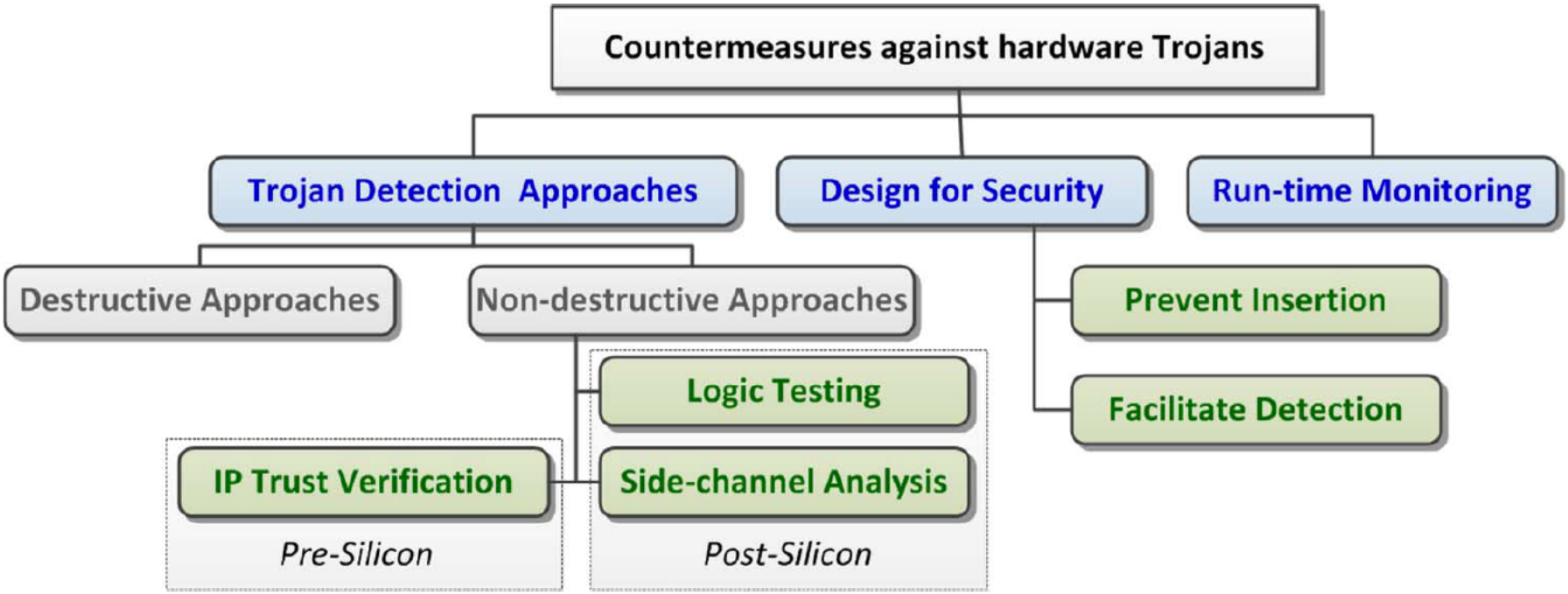
- The write wire can excite the supervisor wire
- A fabrication defect or time bomb can be inserted in the design
- It is possible to trigger the write signal and also activate the supervisor mode







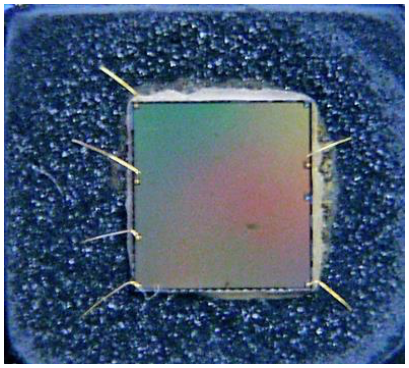
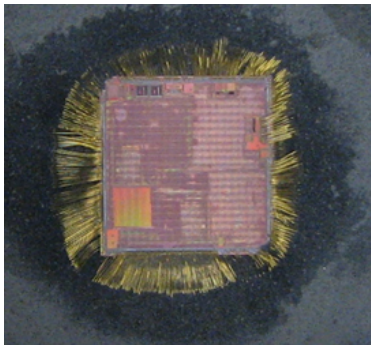
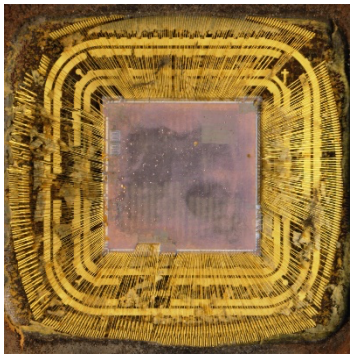
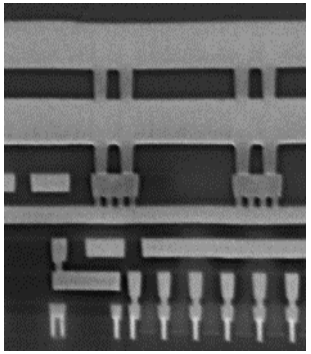
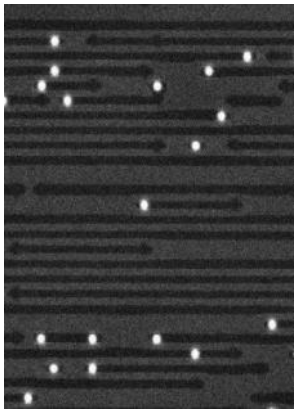
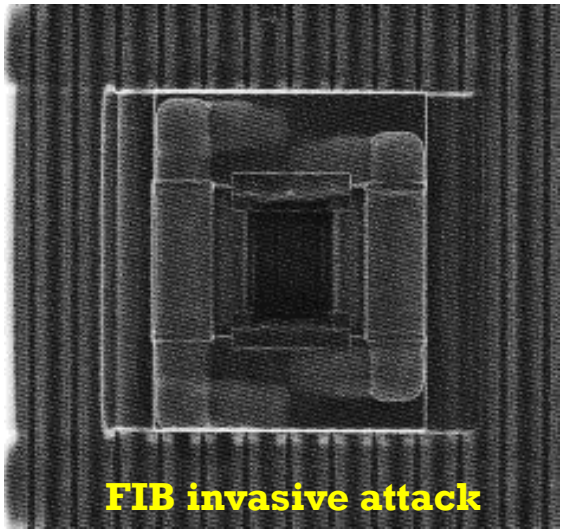
HARDWARE TROJAN MITIGATIONS

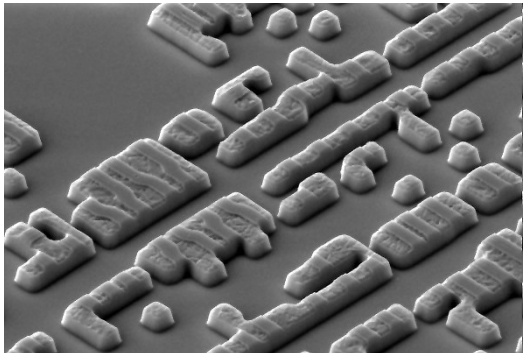
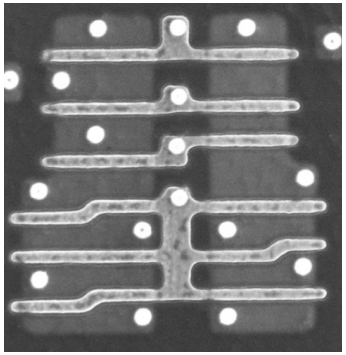
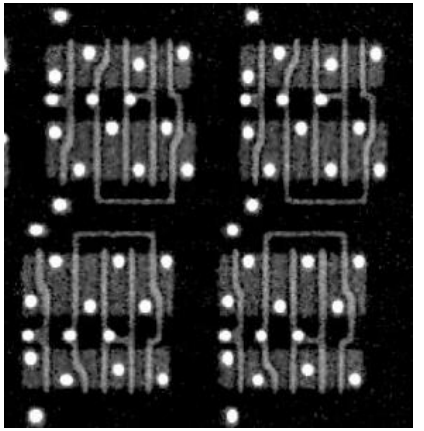


Bhunia *et al.* "Hardware Trojan Attacks: Threat Analysis and Countermeasures," Proc. of IEEE, 2014

REVERSE ENGINEERING

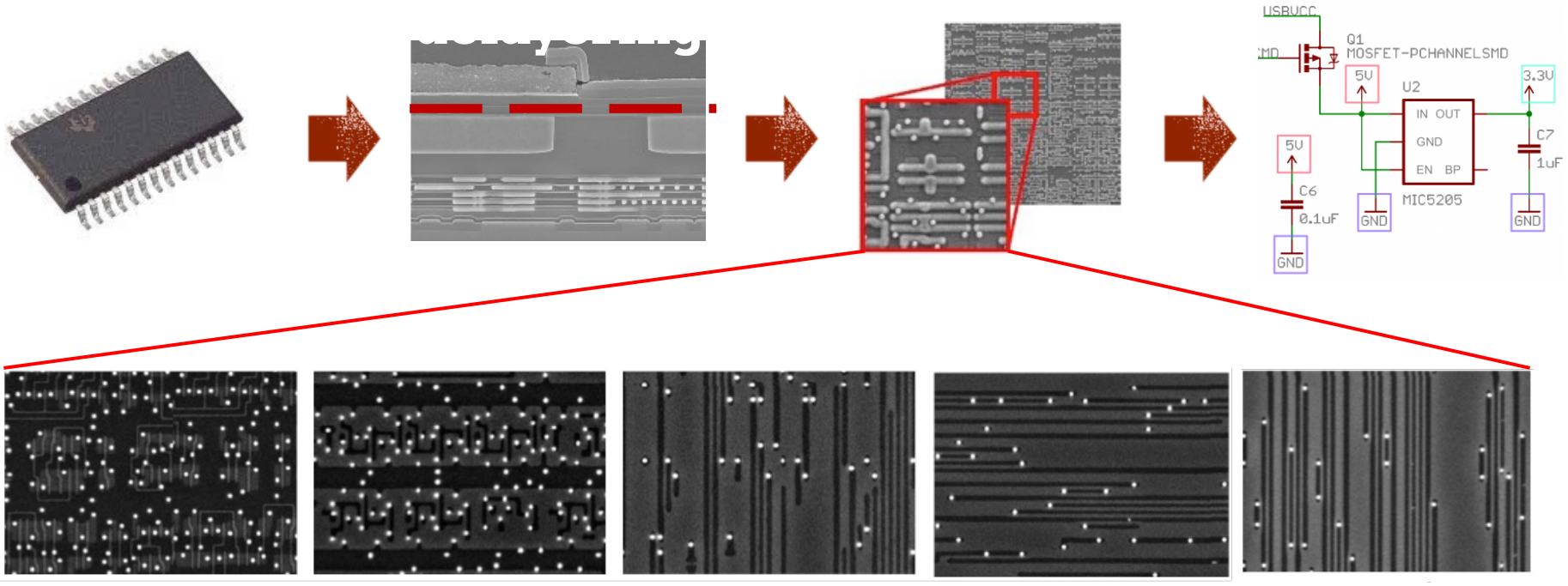
- Reverse engineering is now available commercially

Source: Texplained, *Hardware Security Insight*

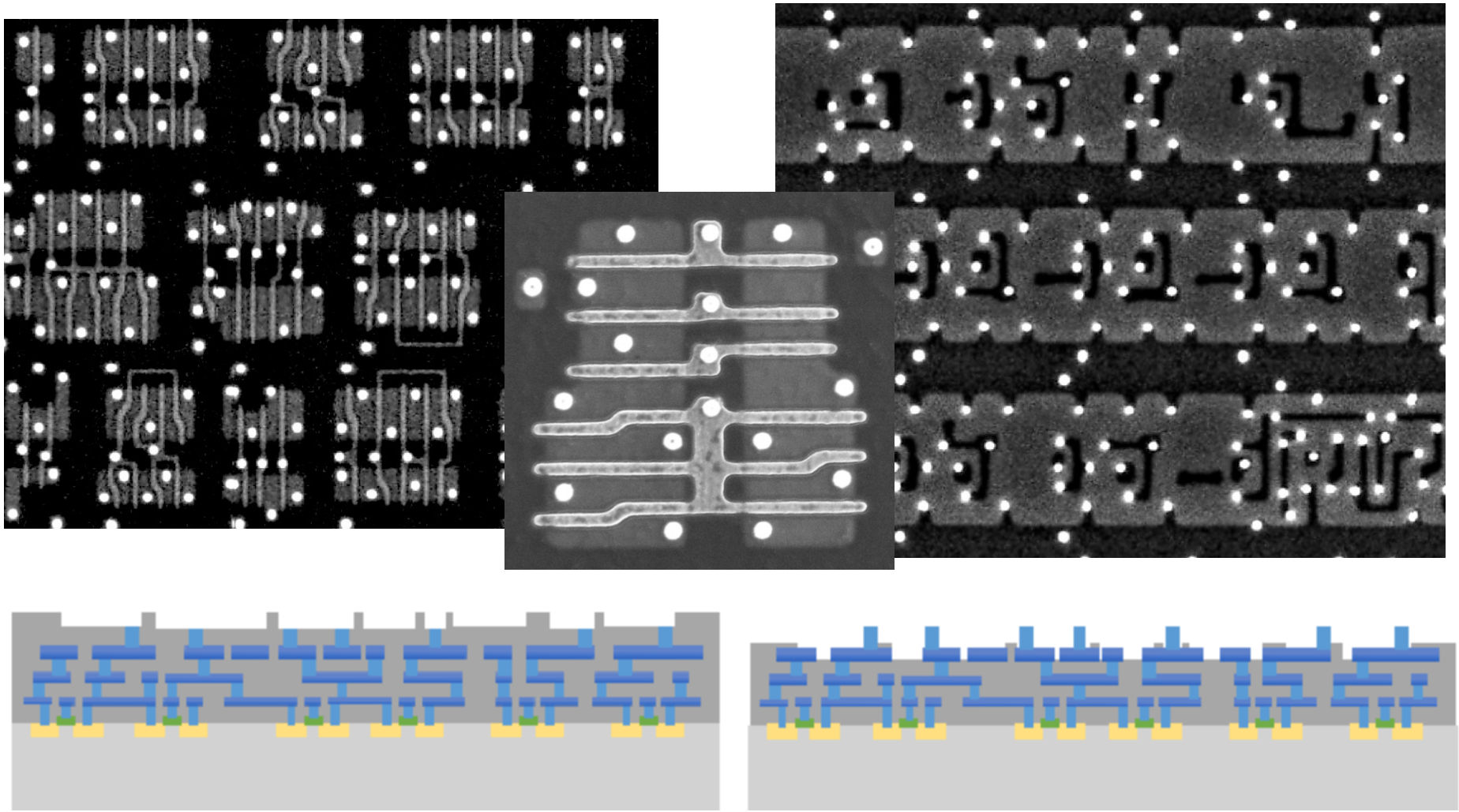
REVERSE ENGINEERING



PIRACY & REVERSE ENGINEERING

- Recovering the IP of a design and using it into different products
  - Producing more chips using an original design from a client
- Recovering the IP within the chip using reverse engineering techniques
  - Depackaging/Delayering: Removing the different metal layers of the IC
  - SEM imaging, annotation, netlist extraction

PIRACY & REVERSE ENGINEERING



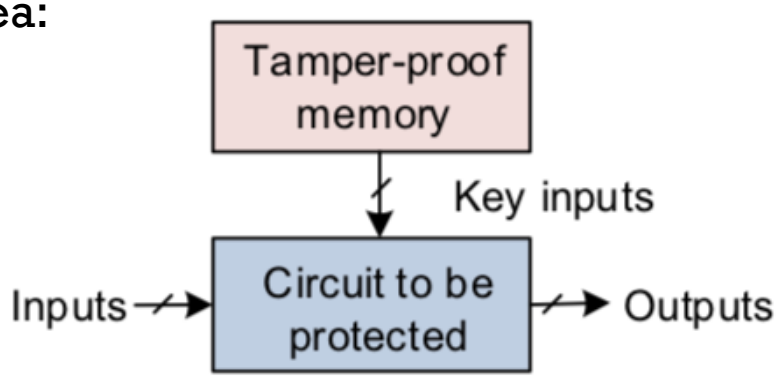
Source: Texplained, *Hardware Security Insight*

PIRACY & REVERSE ENGINEERING

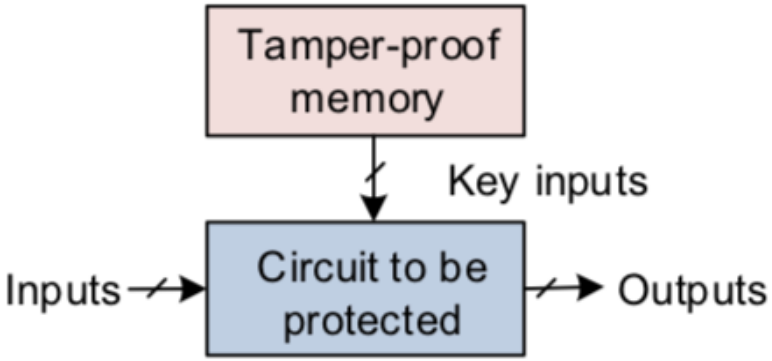
- Increasing cost of IC manufacturing
  - Many fabless companies over the years
  - Outsourced manufacturing, multiple parties
- Global design flow
  - IP protection becomes harder
  - Challenging security threats
  - Piracy, reverse engineering, overbuilding
- Design for Trust (DfTr) techniques
  - Logic locking, split manufacturing, camouflaging

LOGIC LOCKING

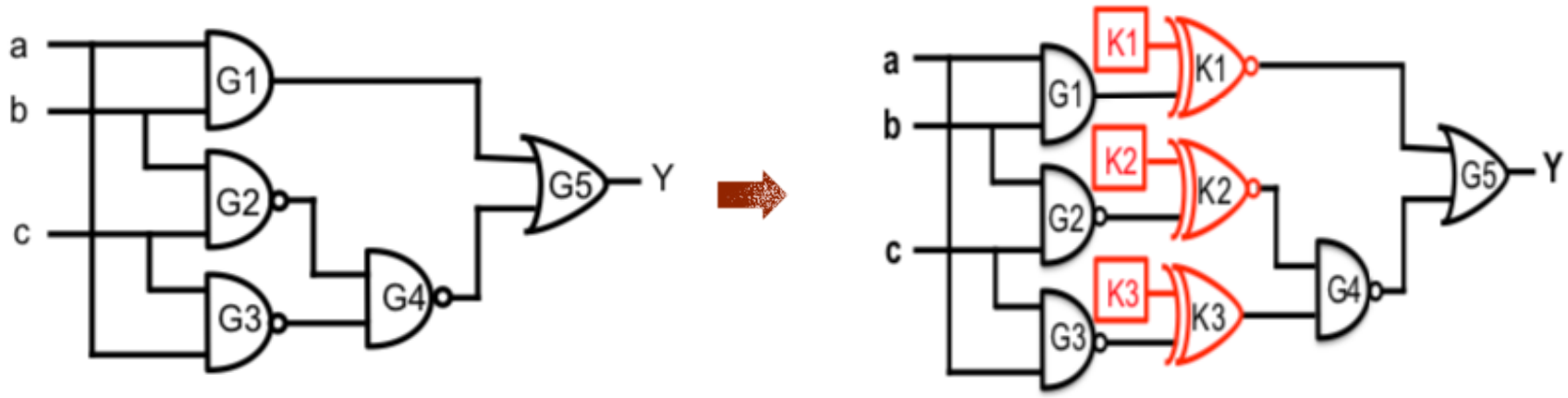
- The designer is trusted
  - All design house personnel are trustworthy
  - All CAD tools are trustworthy
- The Foundry is untrusted
  - Honest-but-curious adversary
  - The foundry wants to reverse engineer (RE), overproduce
- The testing facility is untrusted
  - Access to valid input/output pairs
- The end user is untrusted (RE threat)
- Idea:



LOGIC LOCKING



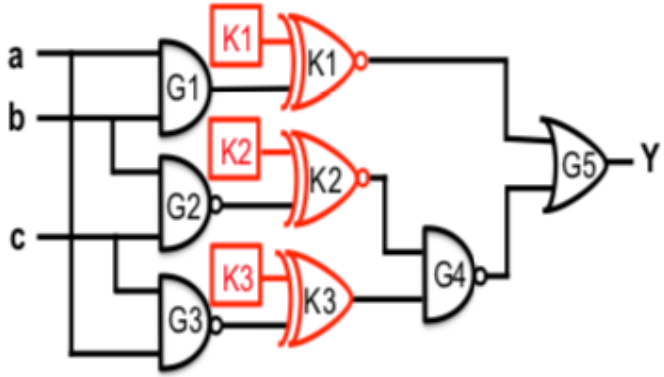
- Insert additional logic
  - XOR gates, XNOR gates, LUTs
  - Uses a secret key
  - Locked circuit has two sets of inputs
    - Original inputs, key inputs



LOGIC LOCKING

- Design flow
  - Orig. circuit -> Key gates -> Locked netlist
  - Fabrication, testing, packaging (untrusted)
  - Activation -> Functional IC
    - Adversary may access the functional IC

- Without secret key:
  - No functional IC
  - No overproduction
  - No reverse engineering, design is protected



- Activation:
  - Load the correct key into tamper-proof memory on the chip
  - The chip becomes functional
  - Receive correct outputs

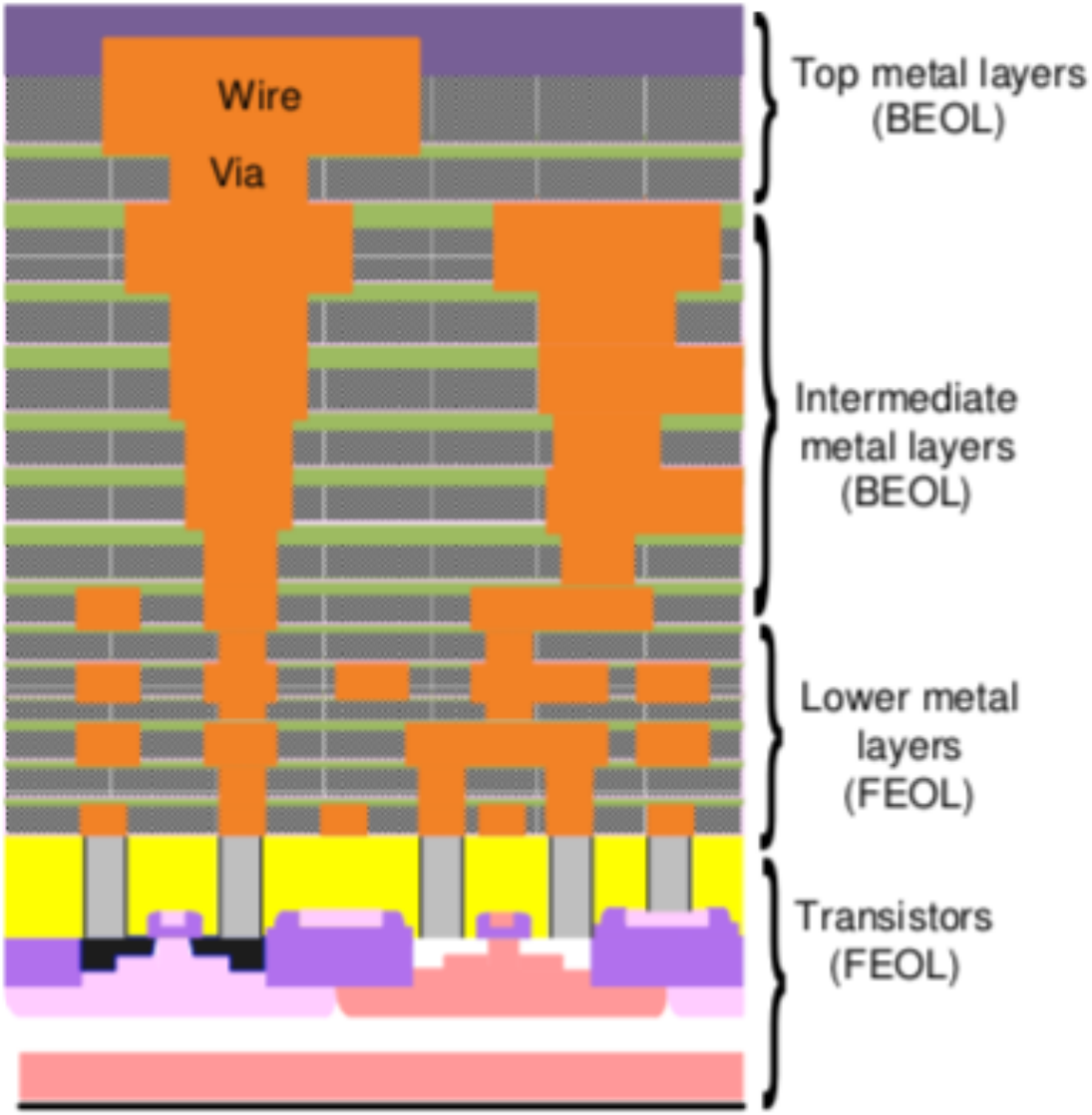
SPLIT MANUFACTURING

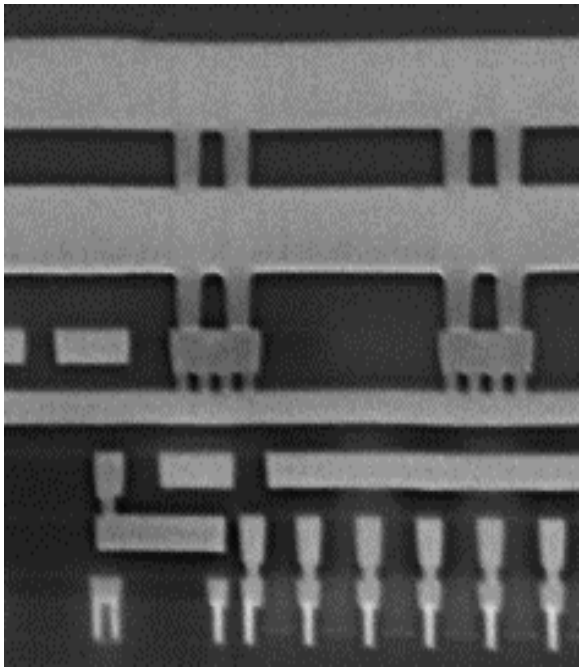
- Protection against overproduction, IP theft, reverse engineering

- The chip is divided into two parts
  - Front End Of Line (FEOL) layers
    - Transistors
    - Lower Metal layers
  - Back End Of Line (BEOL) layers
    - Top Metal layers

- The two different parts are fabricated in different foundries

IC LAYOUT CROSS SECTION



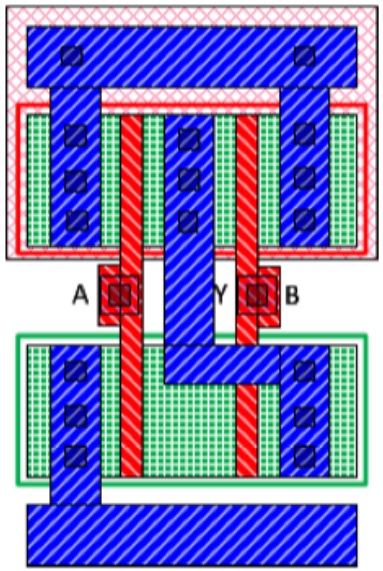


Source: Texplained, *Hardware Security Insight*

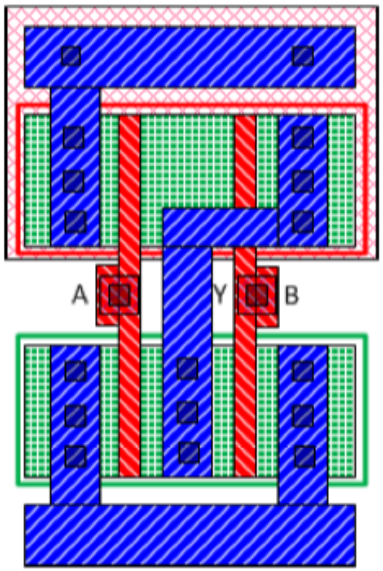
IC CAMOUFLAGING

- Protection against IP theft and RE
  - Use configurable cells in strategic locations
  - Hide design intent
  - Layout similar to other standard cells
  - For example, NAND, NOR or XOR may look identical from a top down angle
  - The attacker cannot learn anything about the design by observing these cells

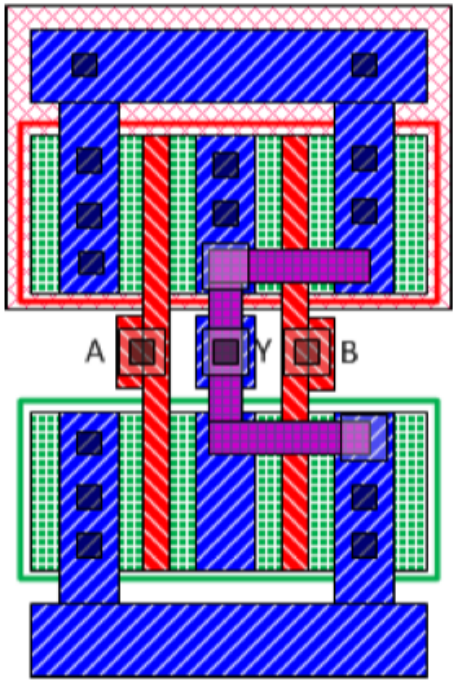
IC CAMOUFLAGING



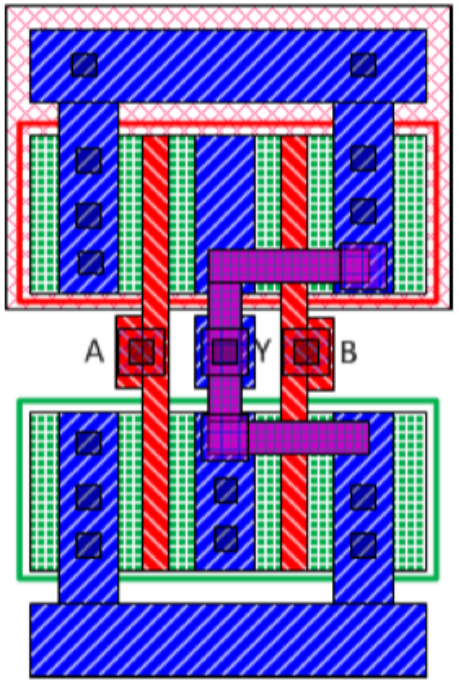
NAND



NOR

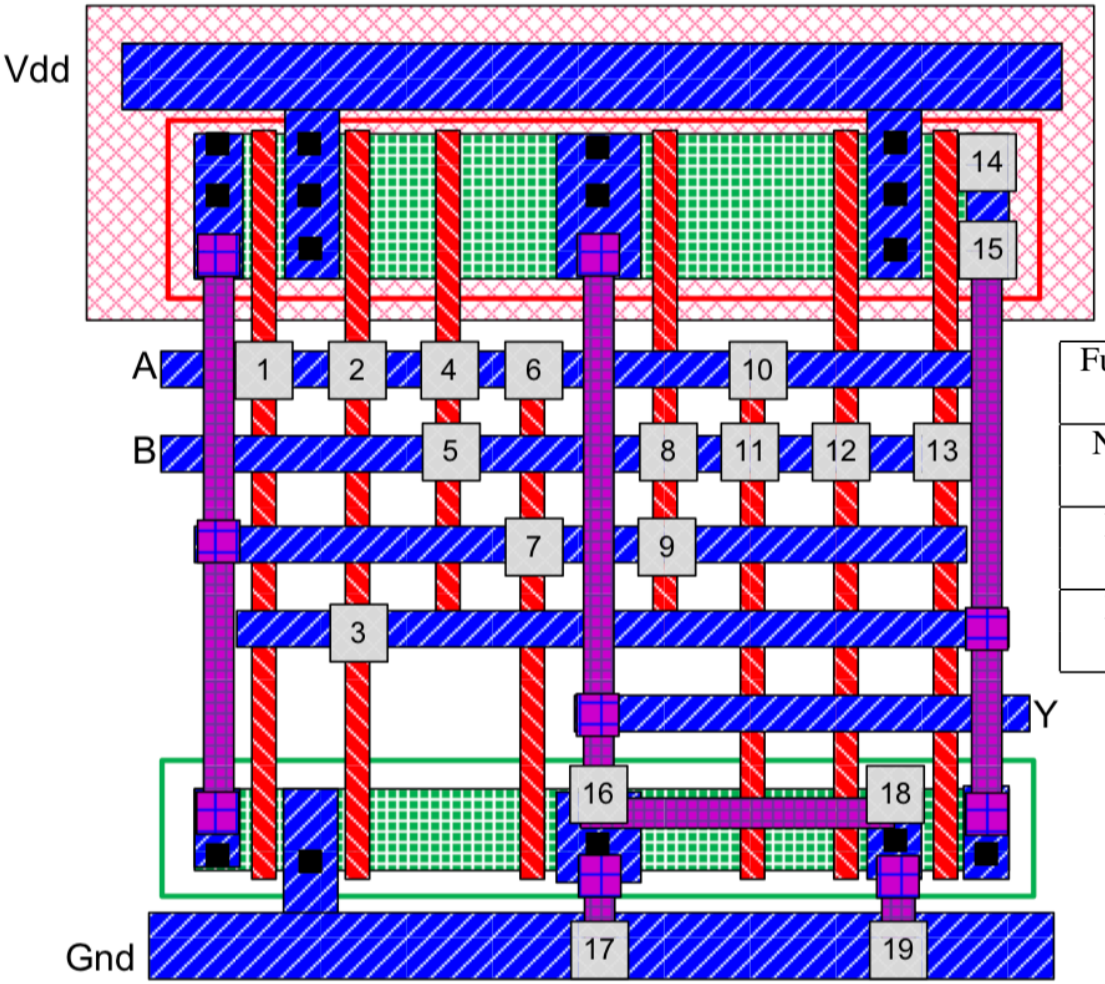


Cmfl-NAND



Cmfl-NOR

IC CAMOUFLAGING



Function	Contacts	
	True	Dummy
NAND	2, 4, 6, 8, 11, 12, 16, 17	1, 3, 5, 7, 9, 10, 13, 14, 15, 18, 19
NOR	2, 5, 6, 11, 12, 18, 19	1, 3, 4, 7, 8, 9, 10, 13, 14, 15, 16, 17
XOR	1, 3, 4, 7, 9, 10, 12, 13, 14, 15, 18, 19	2, 5, 6, 8, 11, 16, 17

Rajendran *et al.* "Security Analysis of Integrated Circuit Camouflaging," CCS, 2013