Protecting Electronics Supply Chain from Design to Resign

Mark M. Tehranipoor

Intel Charles E. Young Preeminence Endowed Chair Professor in Cybersecurity

Florida Institute for Cybersecurity Research

Outline

- Problem Statement and the Fundamentals
- Example Attacks
- Electronics Supply Chain Vulnerabilities
- PUF + ECID
- Counterfeit Electronics
- Logic Obfuscation / IP Encryption
- Hardware Trojans
- Research Challenges

Outline

- Problem Statement and the Fundamentals
- Example Attacks
- Electronics Supply Chain Vulnerabilities
- PUF + ECID
- Counterfeit Electronics
- Logic Obfuscation / IP Encryption
- Hardware Trojans
- Research Challenges

Digital Transformation

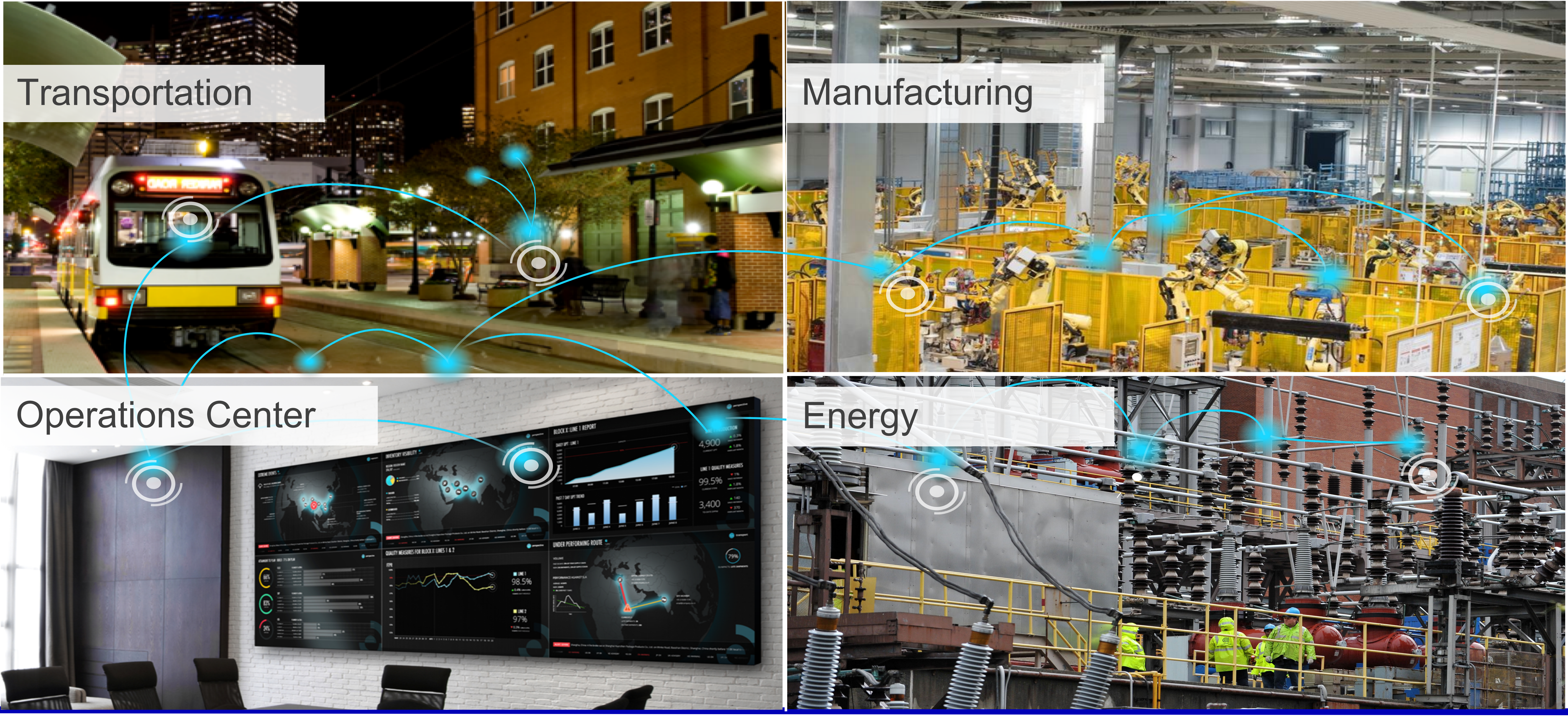
The Impact of Digital Transformation

Operations Technology

Information Technology

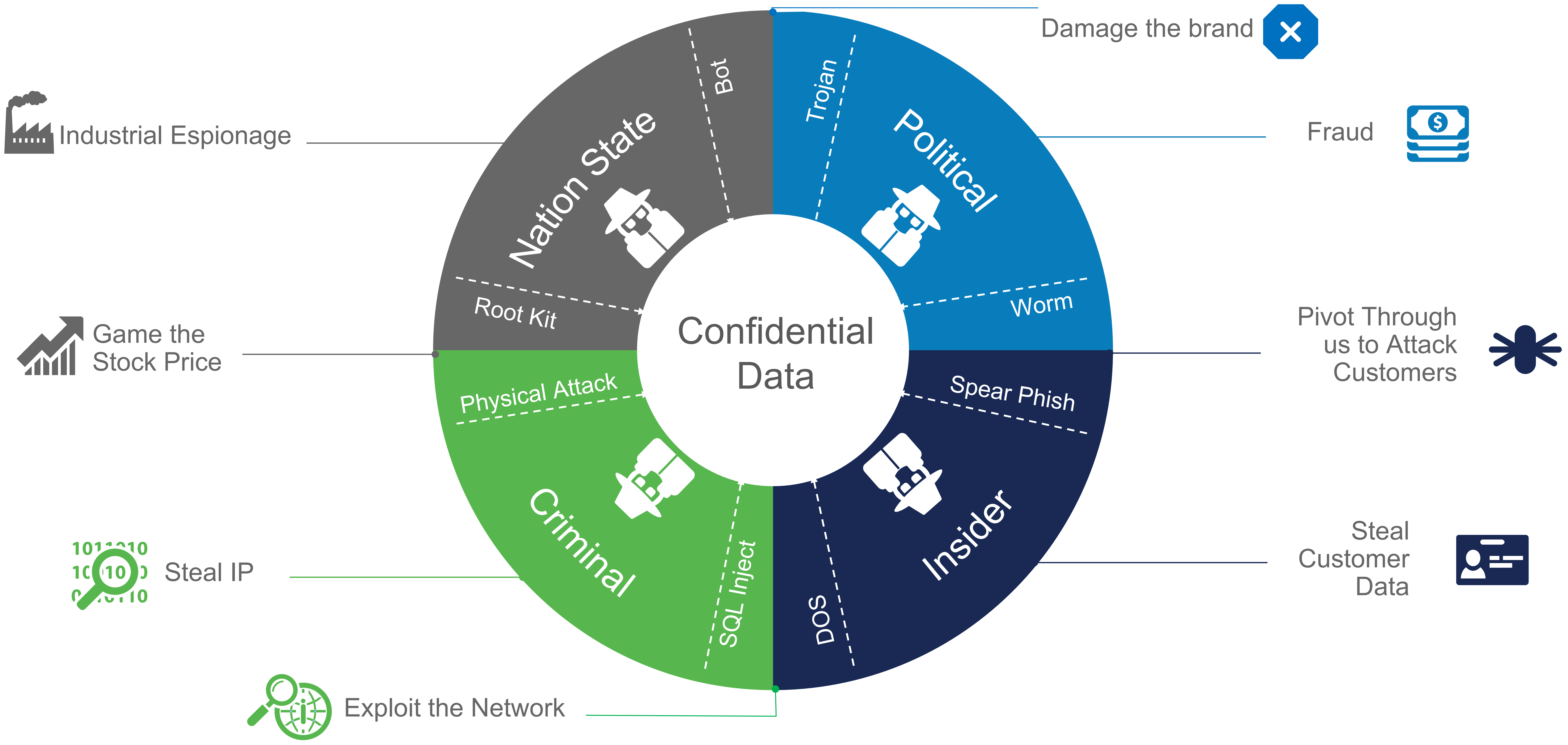
Business Operations ⟷ Enterprise Culture ⟷ 3rd Party Ecosystem

Electronics: The Heart of Digital Transformation

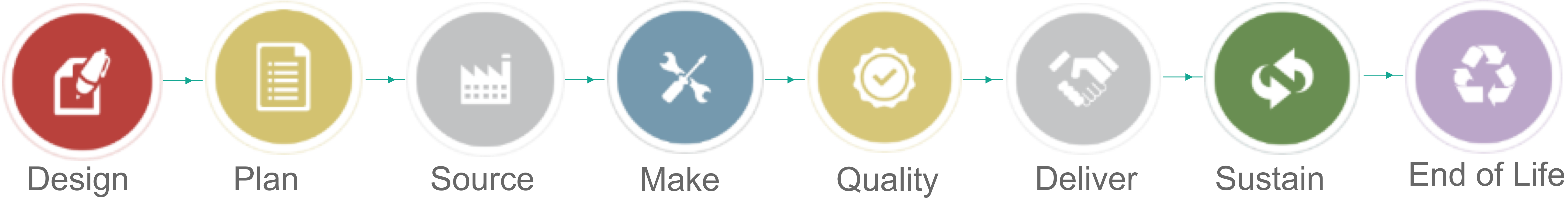


@ Cisco, Edna Conway, RSA 2017

The Fundamentals: Ecosystem Awareness

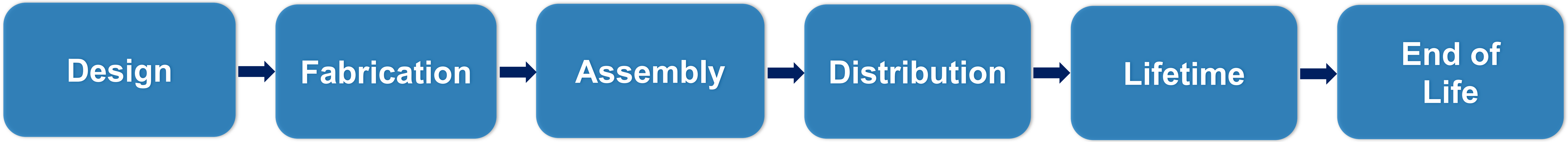


Understand the Information and Communications Value Chain



Design → Plan → Source → Make → Quality → Deliver → Sustain → End of Life

And…
The Electronics Supply Chain Within It



Design → Fabrication → Assembly → Distribution → Lifetime → End of Life

Identify Who/What Is In Your Value Chain

Open Source Software

Software Licensors

HW Component Suppliers

Cloud Service Providers

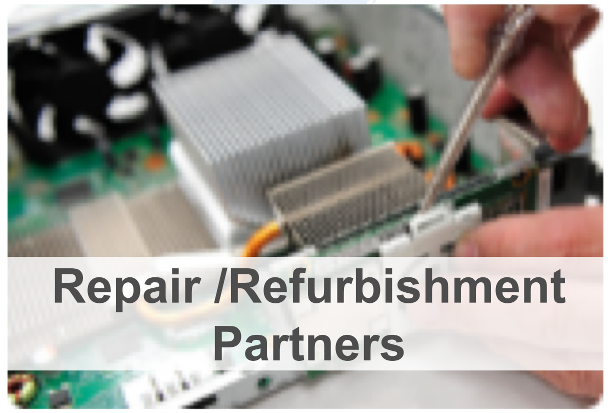
Logistics Partners

OEMs/ODMs

IOT Devices

Manufacturing Partners

Channel/Distributors


Repair /Refurbishment Partners

Scrap Partners

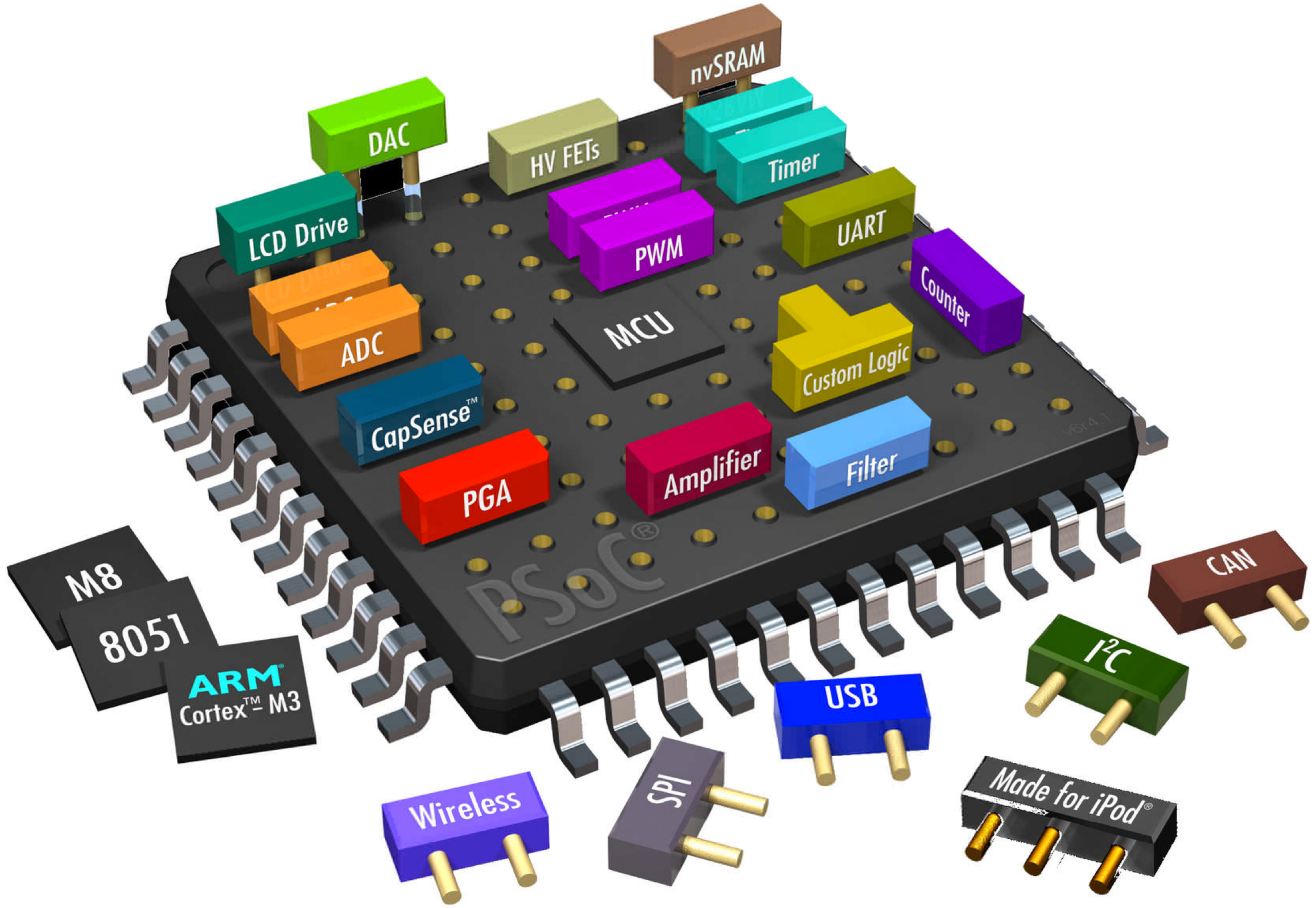
Recycling Partners

@ Cisco, Edna Conway, RSA 2017

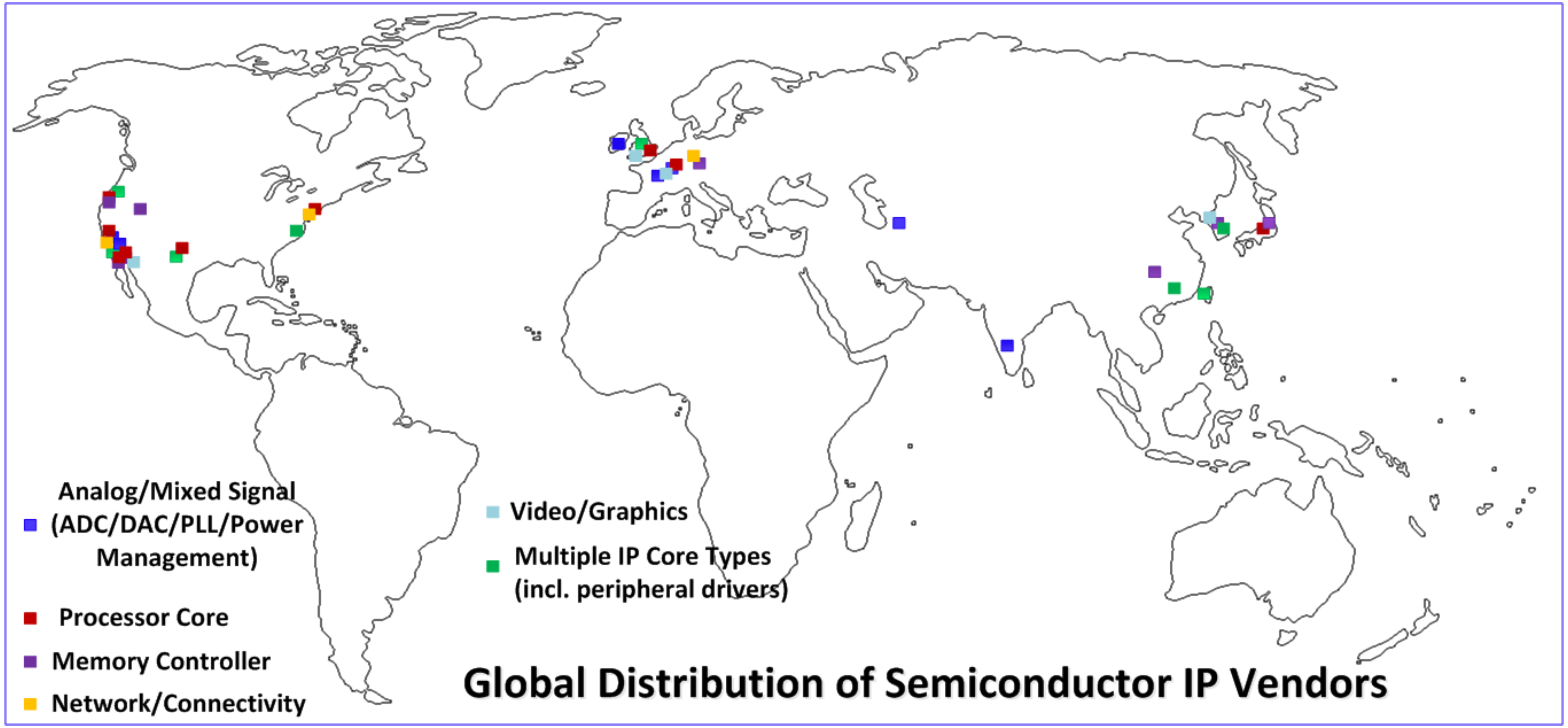
SoC Security

- **Abstraction Level (AL):** Vulnerabilities considered in modular basis at RTL, gate, and physical layout levels

- **System Level (SL):** Vulnerabilities considered from system (e.g., SoC) level perspective – interaction between different cores



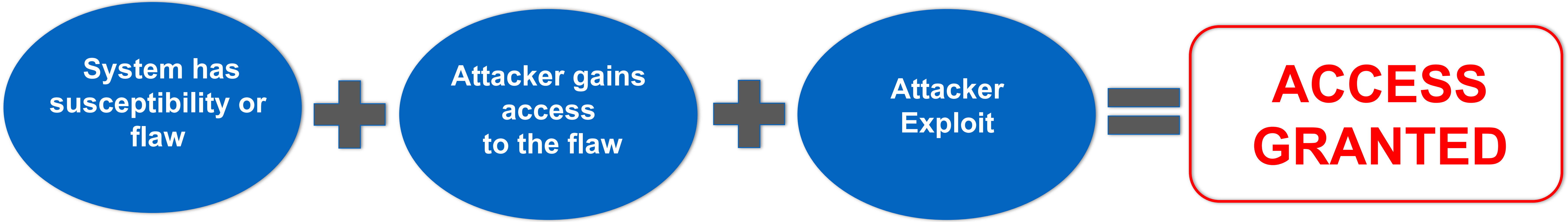
Know Your Supply Chain


🟦 Analog/Mixed Signal (ADC/DAC/PLL/Power Management)
🟥 Processor Core
🟪 Memory Controller
🟨 Network/Connectivity
▨ Video/Graphics
🟩 Multiple IP Core Types (incl. peripheral drivers)

Global Distribution of Semiconductor IP Vendors

Long and globally distributed supply chain of hardware IPs makes SoC design increasingly vulnerable to diverse trust/integrity issues.

The Basics of Vulnerability



System has susceptibility or flaw + Attacker gains access to the flaw + Attacker Exploit = ACCESS GRANTED

REDUCED SYSTEM INFORMATION ASSURANCE

Translate Threats to Exposures

Exposures

Taint

Alteration allowing unauthorized control or content visibility

Counterfeit

Raw materials, finished goods or services which are not authentic

IP Misuse

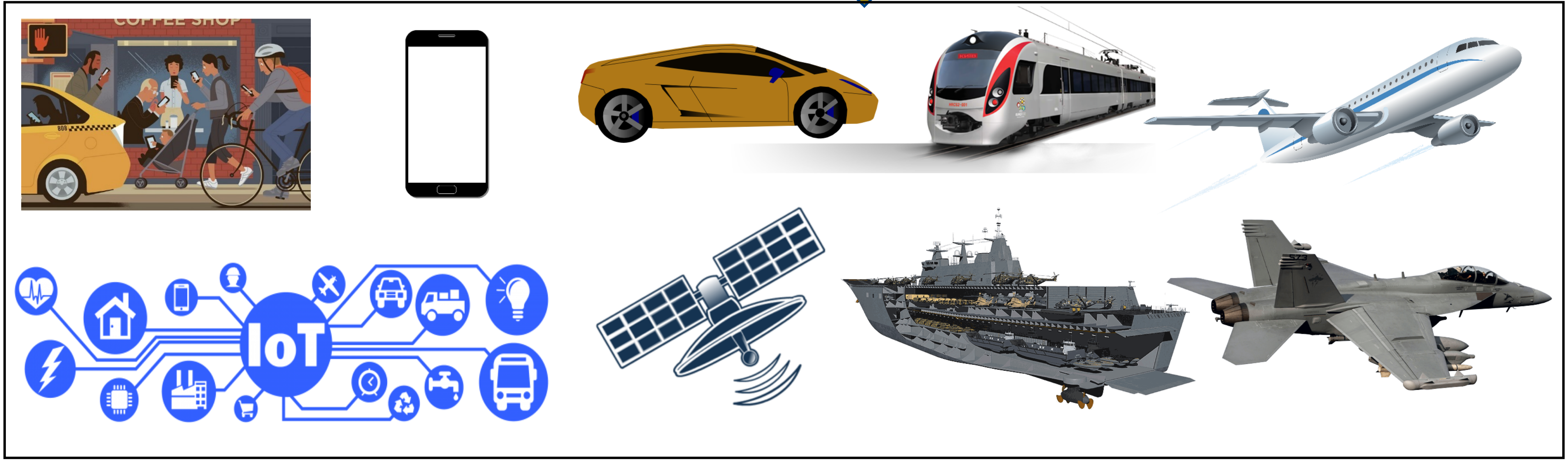
Unauthorized disclosure of intellectual property

Information Security Breach

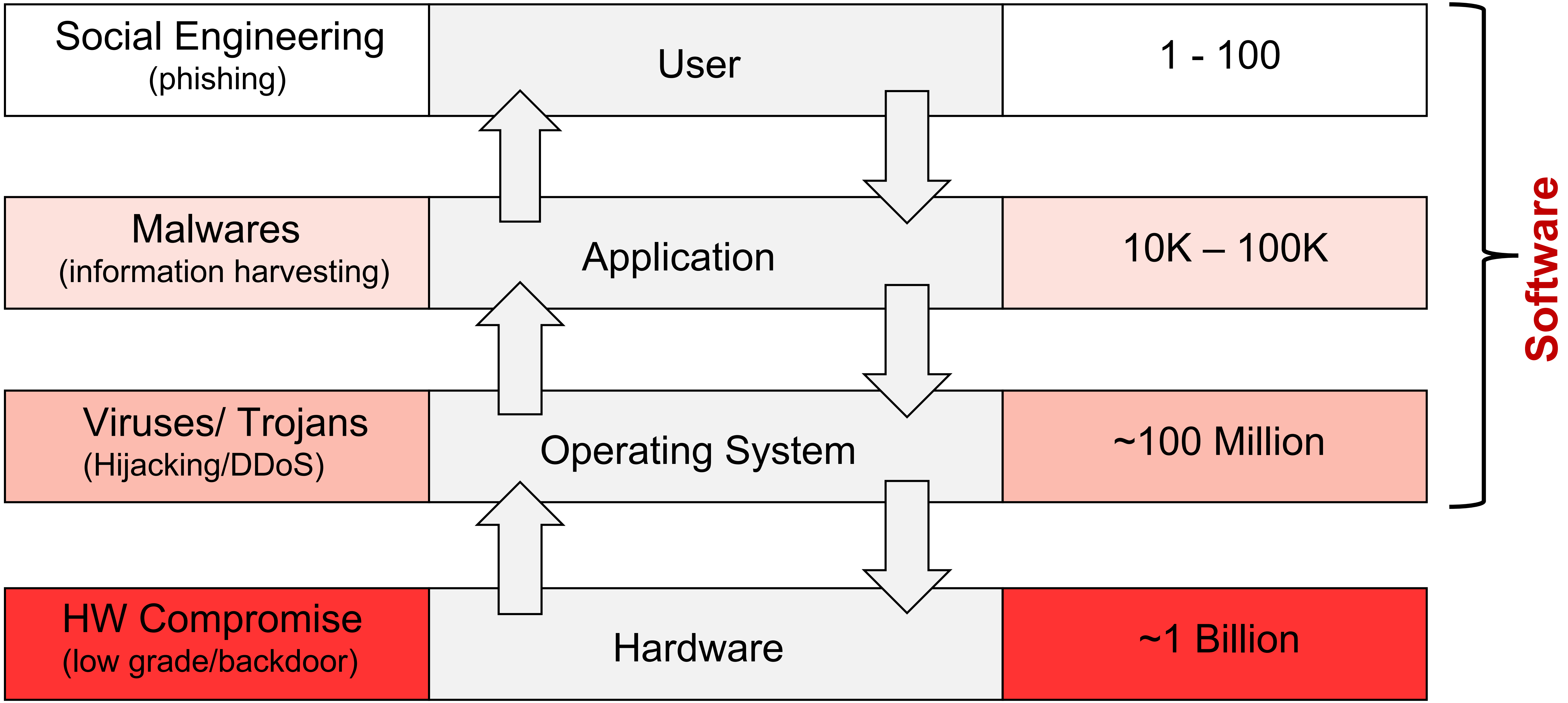
Unauthorized access to confidential information

Applications and Threats

Millions of chips are fabricated and tested in untrusted foundries, assemblies, and are currently in the supply chains



Impact of Hardware Compromise



Attack Types		Relative Impact
Social Engineering (phishing)	User	1 - 100
Malwares (information harvesting)	Application	10K – 100K
Viruses/ Trojans (Hijacking/DDoS)	Operating System	~100 Million
HW Compromise (low grade/backdoor)	Hardware	~1 Billion

Outline

- Problem Statement and the Fundamentals
- Example Attacks
- Supply Chain Vulnerabilities
- PUF + ECID
- Counterfeit Electronics
- Logic Obfuscation / IP Encryption
- Hardware Trojans
- Research Challenges

Example Attacks

Roy Zoppoth stands over a Xerox 914 copy machine, the world's first, which was used in soviet embassies all over the world. The machine was so complex that the CIA used a tiny camera designed by Zoppoth to capture documents copied on the machine by the soviets and retrieved them using a "Xerox repairman" right under the eyes of soviet security.

Photo from edit international courtesy of Roy Zoppoth

Example Attacks

One Printer, One Virus, One Disabled Air Defense

Air defenses knocked out by the secret activation of code smuggled though in commercial hardware. This was back in 1991 and the first Iraq War, when the knockout blow was administered by a virus carried by a printer

Pentagon’s ‘Kill Switch': Urban Myth?

The Pentagon is worried that "backdoors" in computer processors might leave the American military vulnerable to an instant electronic shut-down. Those fears only grew, after an Israeli strike on an alleged nuclear facility in Syria. Many speculated that Syrian air defenses had been sabotaged by chips with a built-in ‘kill switch" — commercial off-the-shelf microprocessors in the Syrian radar might have been purposely fabricated with a hidden “backdoor” inside. By sending a preprogrammed code to those chips, an unknown antagonist had disrupted the chips’ function and temporarily blocked the radar."

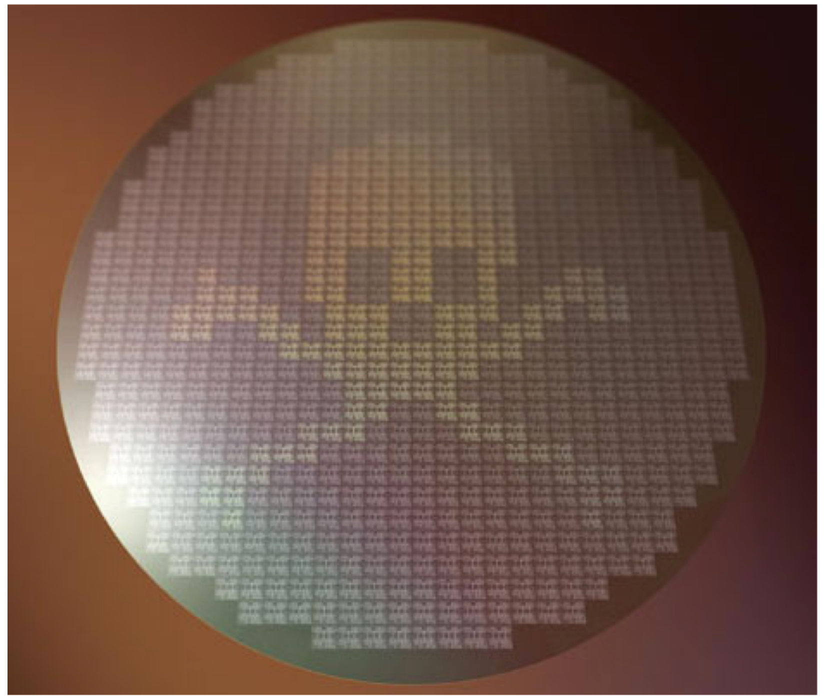
Example Attacks

DHS: Imported Consumer Tech Contains Hidden Hacker Attack Tools

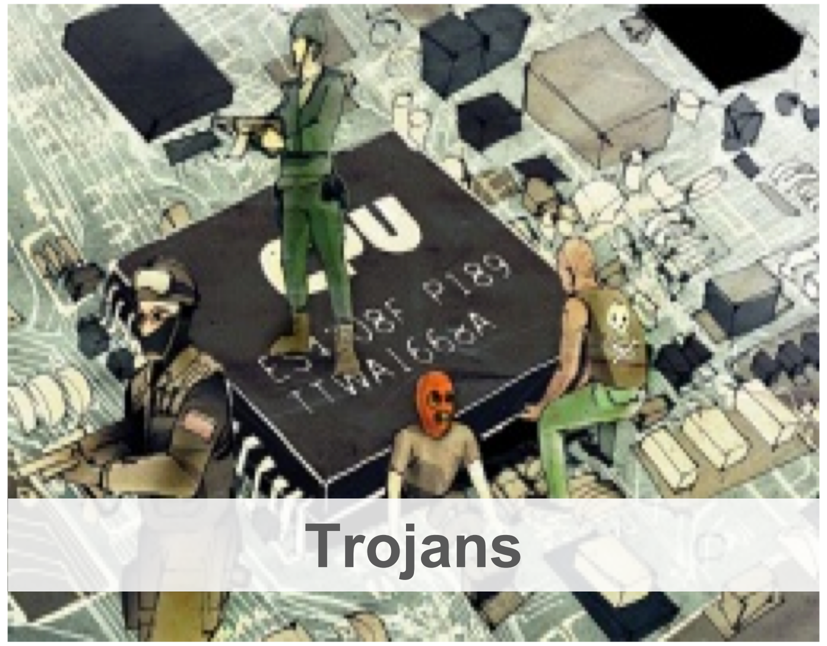
- Top homeland securities have admitted instances where along with software, hardware components that are being imported from foreign parties and used in different US systems are being compromised and altered to enable easier cyber-attacks.

The Hunt for Kill Switch, IEEE Spectrum 2008

- Increasing threat to hardware due to globalization
- Extremely difficult to detect kill switches (utilized by enemies to damage/destroy opponent artillery during critical missions) as well as intentional backdoors (to enable remote control of chips without user knowledge), which may have huge consequences
- Example: Syrian’s Radar during Israeli attack, French Government using kill switches intentionally as a form of active defense to damage the chips if they fall in hostile hands, and more...

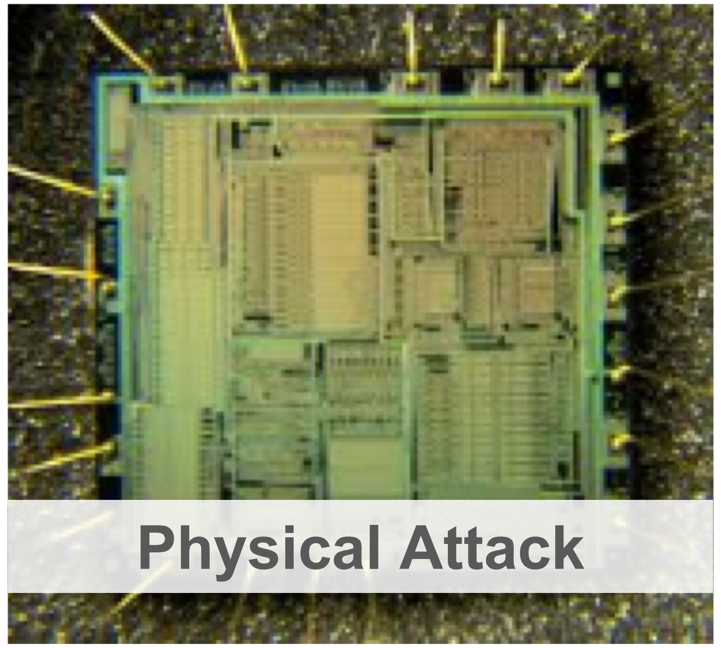


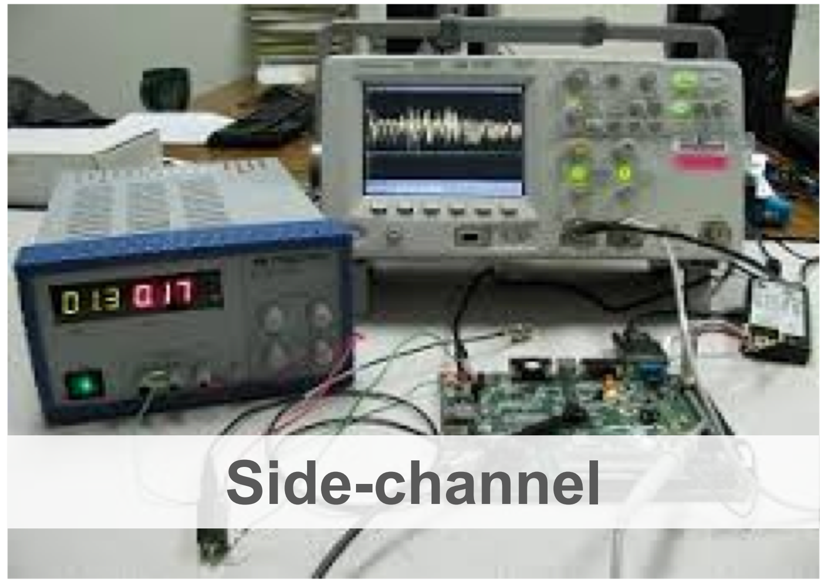
Security Attacks on Hardware

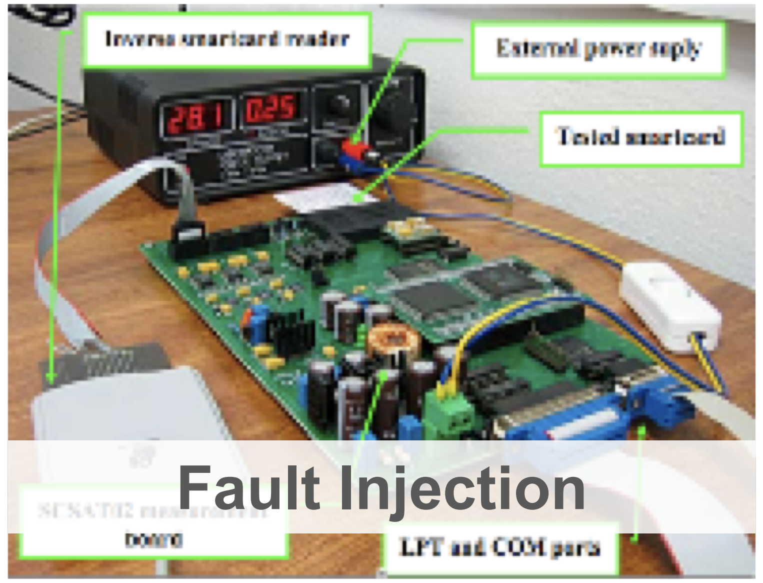

Trojans

Untrusted Foundry

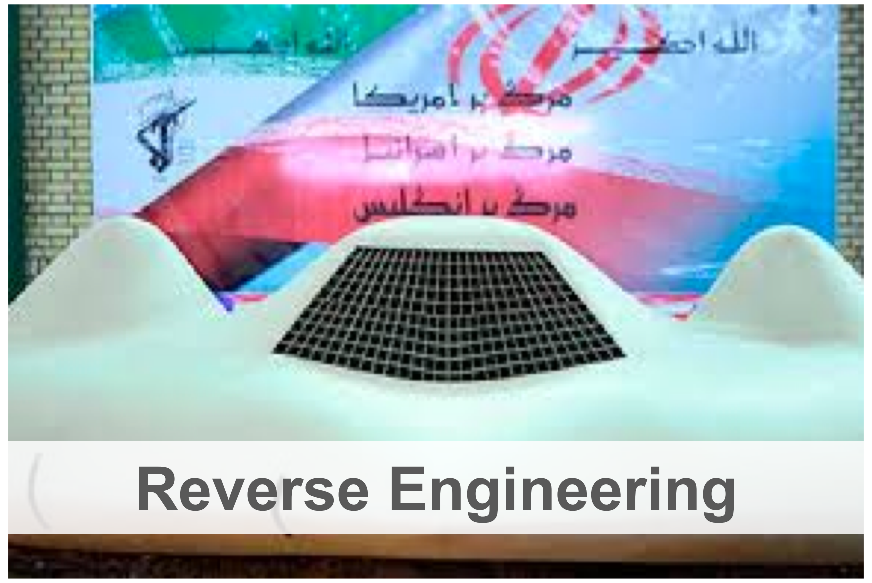
Counterfeit ICs


Physical Attack

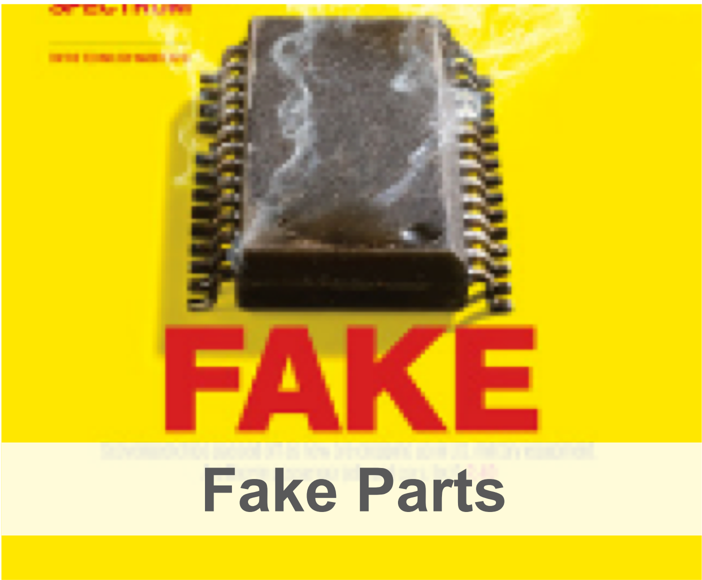

Side-channel



Fault Injection

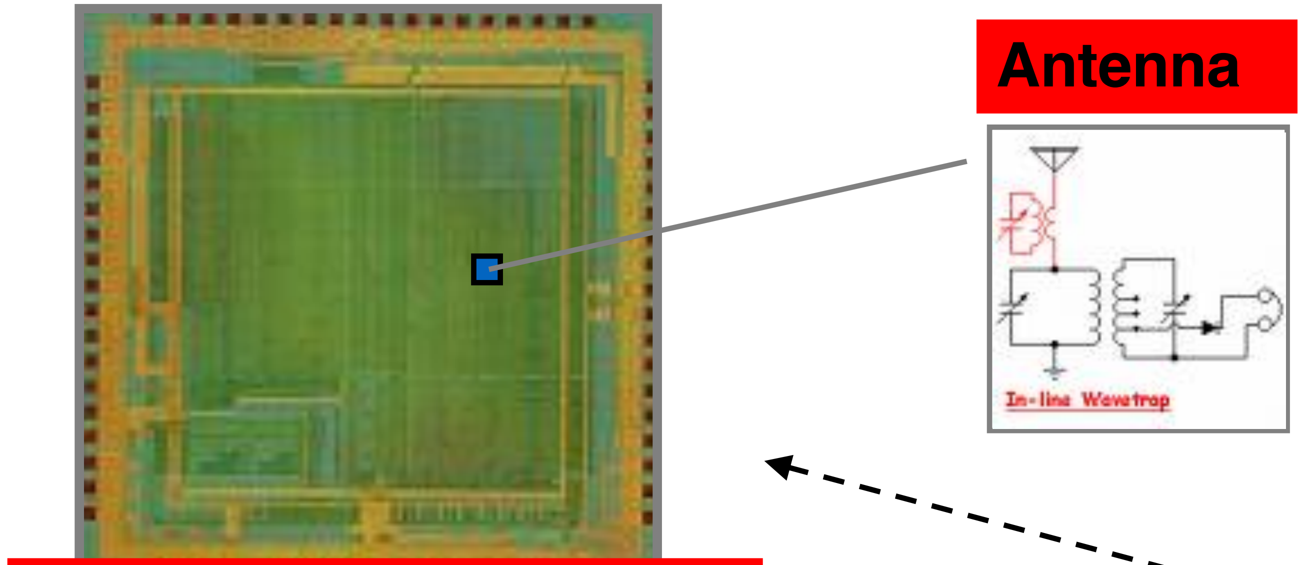


Reverse Engineering



Fake Parts

Hardware Trojan – Back Door



Antenna

Untrusted Hardware

- Adversary can place an Antenna on the fabricated chip.
- Such Trojan cannot be detected since it does not change the functionality of the circuit.

- Adversary can send and receive secret information.
- Adversary can disable the chip, blowup the chip, send wrong processing data, impact circuit information etc.

Hardware Trojan – Time Bomb

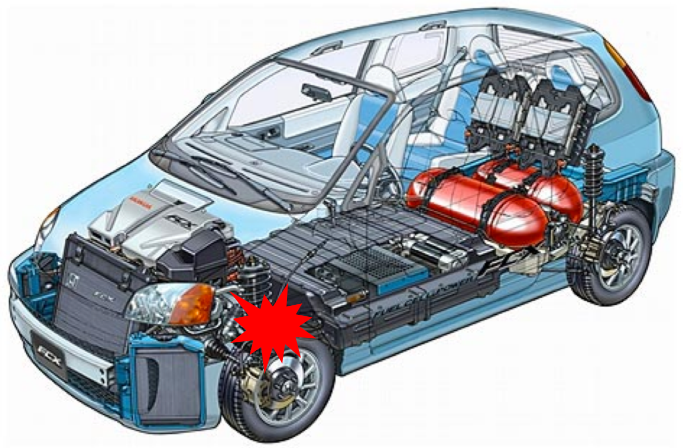
Untrusted Hardware

Counter

Finite state machine (FSM)

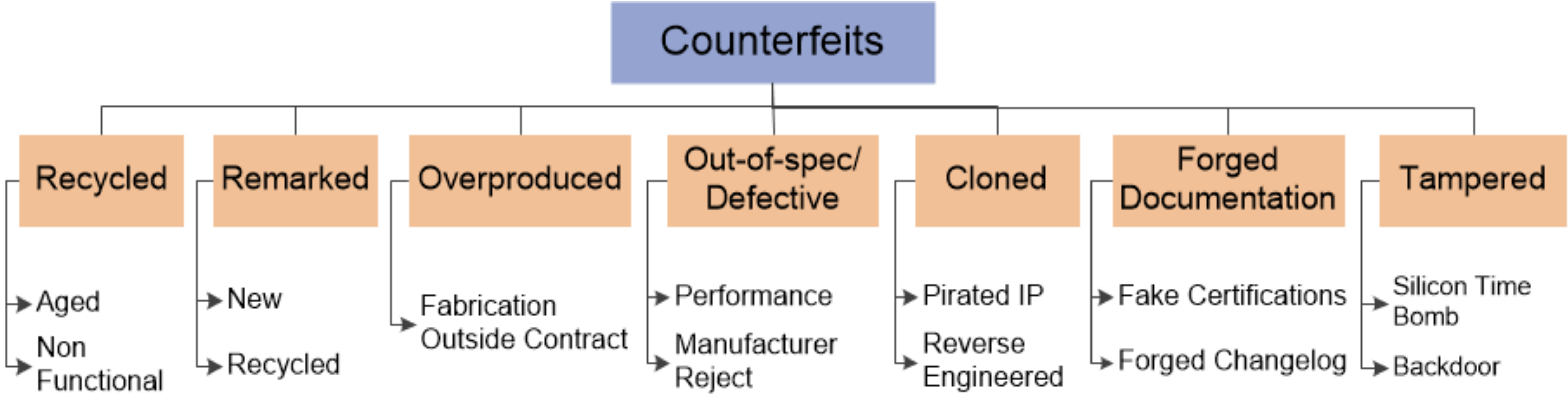
Comparator to monitor key data

Wires/transistors that violate design rules



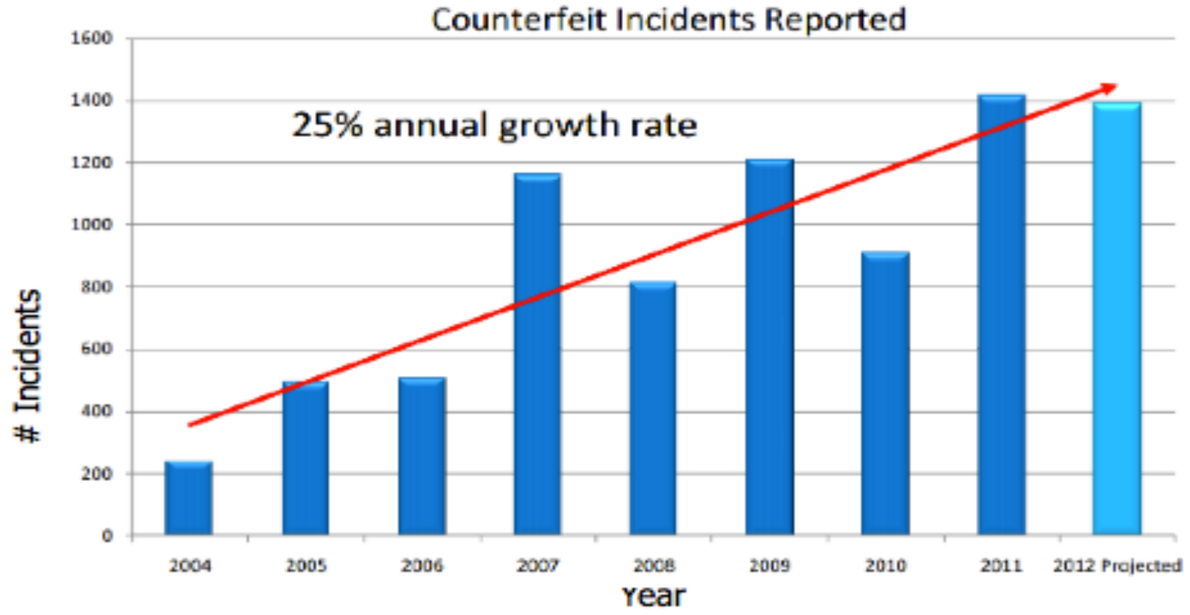
- Such Trojan cannot be detected since it does not change the functionality of the circuit.
- In some cases, adversary has little control on the exact time of Trojan action
- Cause reliability issue

Counterfeit Incidents



Counterfeits

- Recycled
  - Aged
  - Non Functional
- Remarked
  - New
  - Recycled
- Overproduced
  - Fabrication Outside Contract
- Out-of-spec/ Defective
  - Performance
  - Manufacturer Reject
- Cloned
  - Pirated IP
  - Reverse Engineered
- Forged Documentation
  - Fake Certifications
  - Forged Changelog
- Tampered
  - Silicon Time Bomb
  - Backdoor



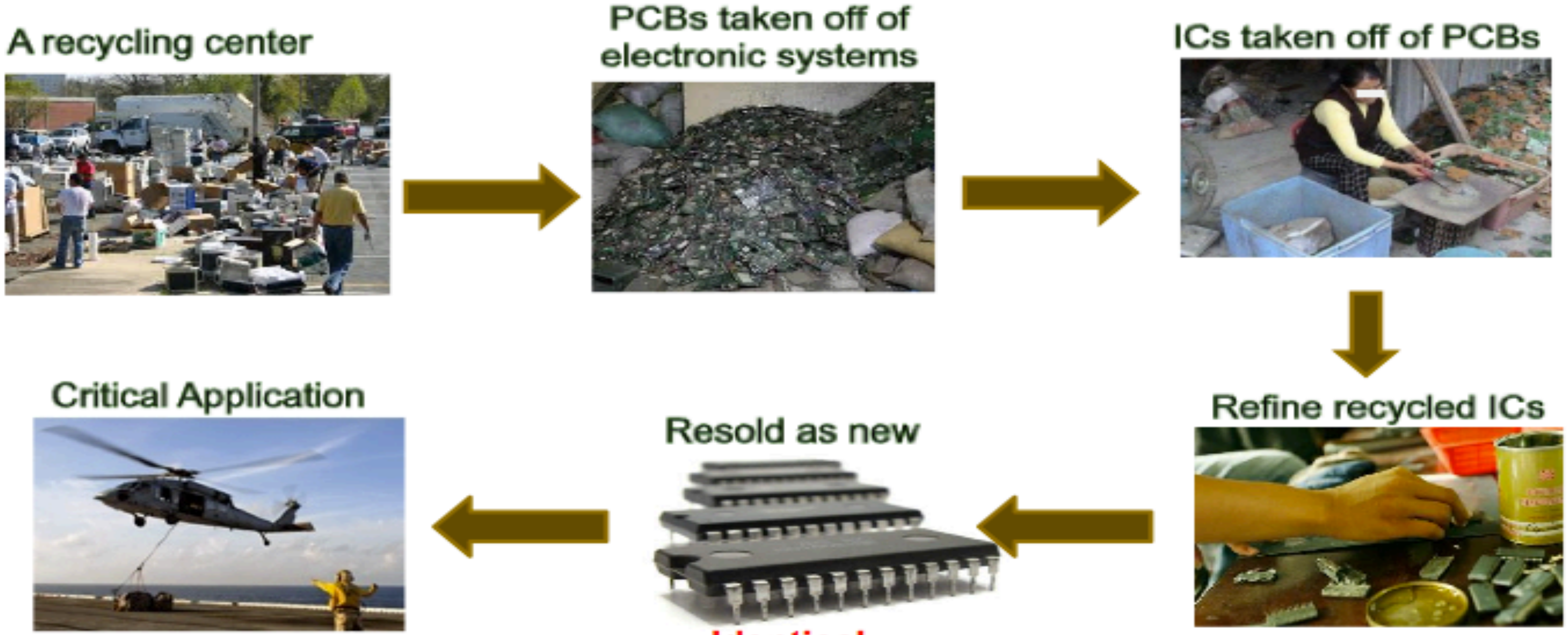
NDAA 2012

Reported counterfeit incidents are growing rapidly since 2009.

Electronics companies loses $100 billion dollar every year because of counterfeiting

U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead," Journal of Electronic Testing: Theory and Applications (JETTA), 2014.

Recycling Process



A recycling center

PCBs taken off of electronic systems

ICs taken off of PCBs

Refine recycled ICs

Resold as new

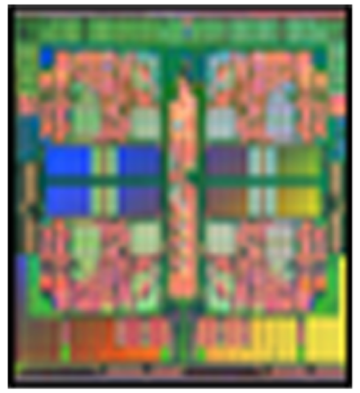
Critical Application

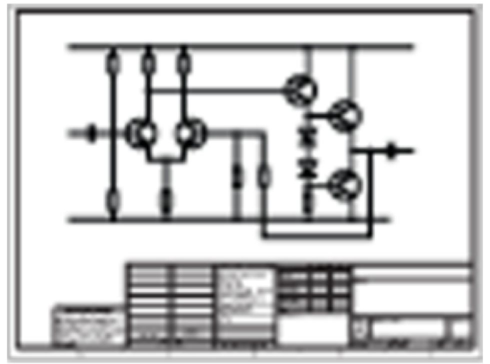
Identical:
Appearance, Function, Specification

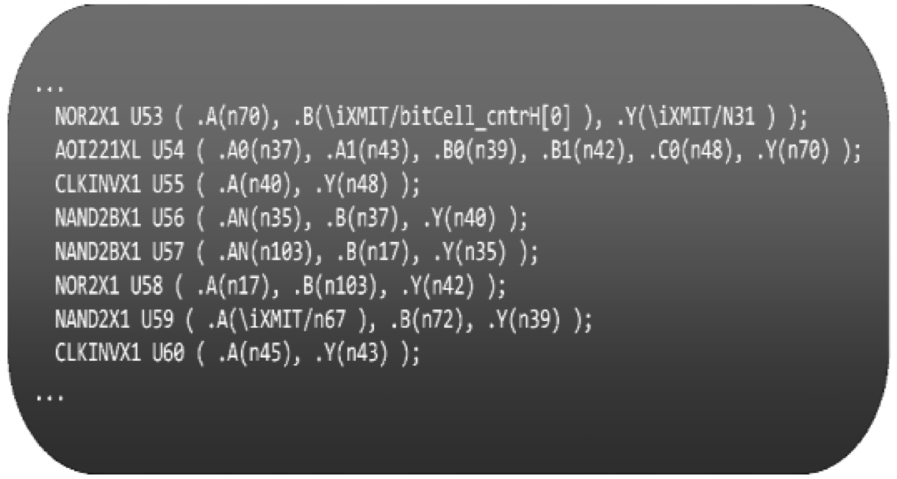
Consumer trends suggest that more gadgets are used in much shorter time – more e-waste

Source: Images are taken from google

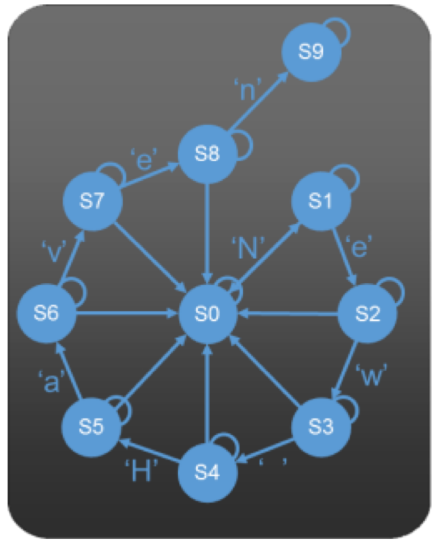
Chip Reverse Engineering







```
...
  NOR2X1 U53 ( .A(n70), .B(\iXMIT/bitCell_cntrH[0] ), .Y(\iXMIT/N31 ) );
  AOI221XL U54 ( .A0(n37), .A1(n43), .B0(n39), .B1(n42), .C0(n48), .Y(n70) );
  CLKINVX1 U55 ( .A(n40), .Y(n48) );
  NAND2BX1 U56 ( .AN(n35), .B(n37), .Y(n40) );
  NAND2BX1 U57 ( .AN(n103), .B(n17), .Y(n35) );
  NOR2X1 U58 ( .A(n17), .B(n103), .Y(n42) );
  NAND2X1 U59 ( .A(\iXMIT/n67 ), .B(n72), .Y(n39) );
  CLKINVX1 U60 ( .A(n45), .Y(n43) );
...
```



Stay Aware

FT FINANCIAL TIMES

‘Internet of things’ was mobilised for internet outage, says Dyn

npr

'Internet Of Things' Hacking Attack Led To Widespread Outage Of Popular Websites

THE HILL

Counterfeit electronics: Another security threat from China

EETimes

Obama to Sign Bill Combating Counterfeit Chips

COALITION FOR AMERICAN ElectronicsRecycling

Unregulated E-waste Exports Fuel Counterfeit Electronics That Undermine U.S. National Security

PCWorld

Hackers create more IoT botnets with Mirai source code

THE HILL

House panel to tackle security of internet-connected devices

Forbes

World's Biggest Mirai Botnet Is Being Rented Out For DDoS Attacks

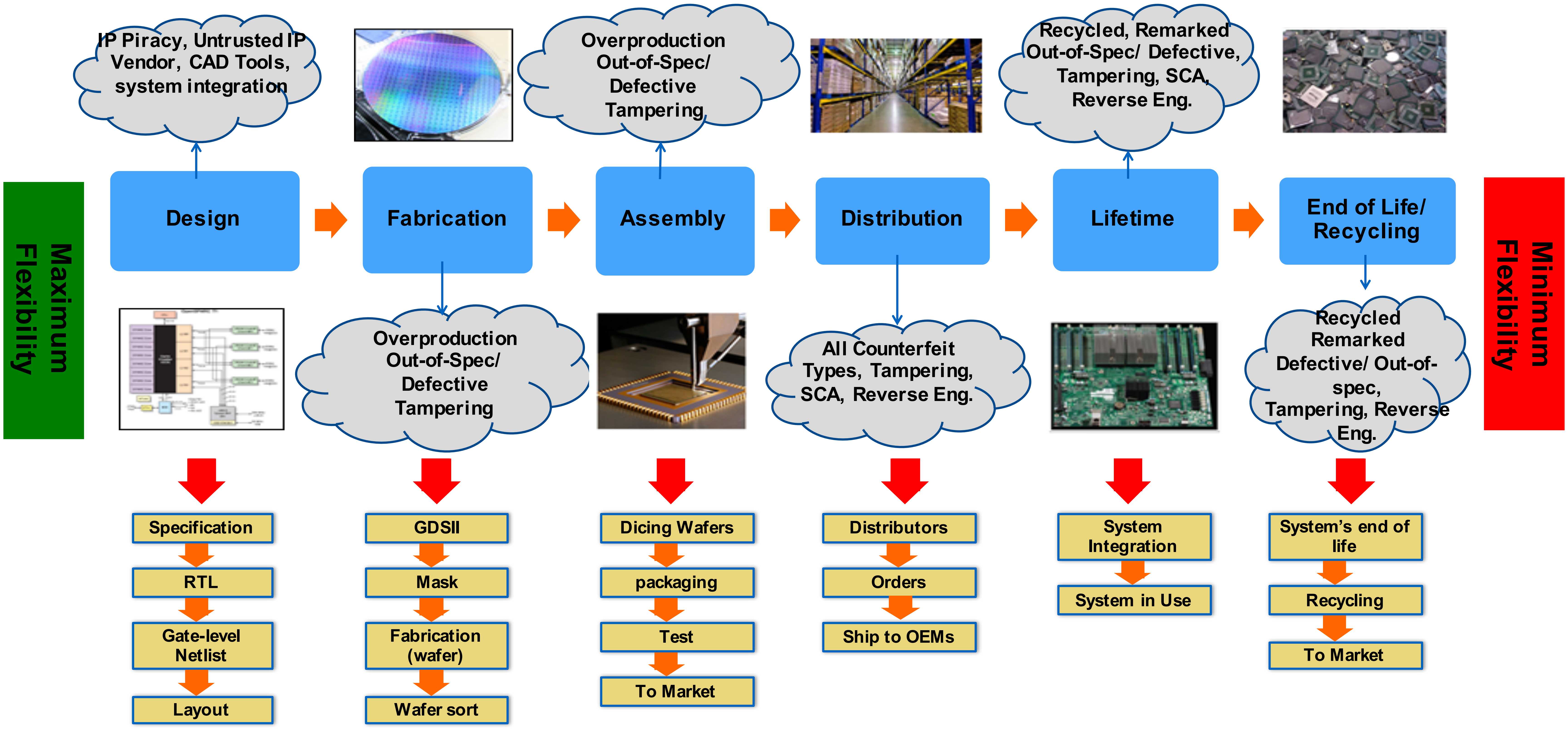
cyberscoop

After Dyn cyberattack, lawmakers seek best path forward

Outline

- Problem Statement and the Fundamentals
- Example Attacks
- Electronics Supply Chain Vulnerabilities
- PUF + ECID
- Counterfeit Electronics
- Logic Obfuscation / IP Encryption
- Hardware Trojans
- Research Challenges

IC and System Supply Chain Vulnerability



Maximum Flexibility

Design

IP Piracy, Untrusted IP Vendor, CAD Tools, system integration

Specification → RTL → Gate-level Netlist → Layout

Fabrication

Overproduction Out-of-Spec/ Defective Tampering

GDSII → Mask → Fabrication (wafer) → Wafer sort

Assembly

Overproduction Out-of-Spec/ Defective Tampering

Dicing Wafers → packaging → Test → To Market

Distribution

All Counterfeit Types, Tampering, SCA, Reverse Eng.

Distributors → Orders → Ship to OEMs

Lifetime

Recycled, Remarked Out-of-Spec/ Defective, Tampering, SCA, Reverse Eng.

System Integration → System in Use

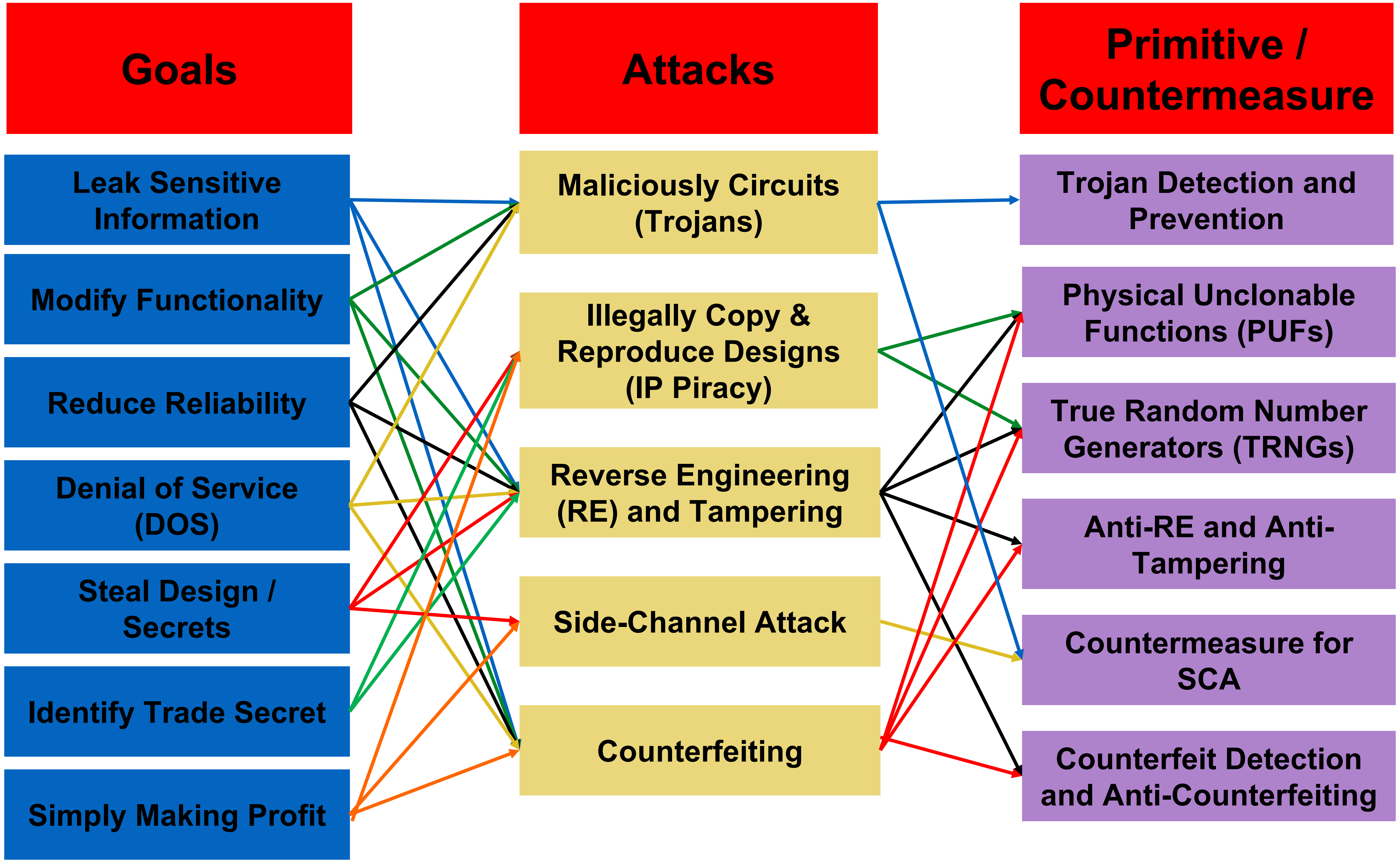
End of Life/ Recycling

Recycled Remarked Defective/ Out-of-spec, Tampering, Reverse Eng.

System's end of life → Recycling → To Market

Minimum Flexibility

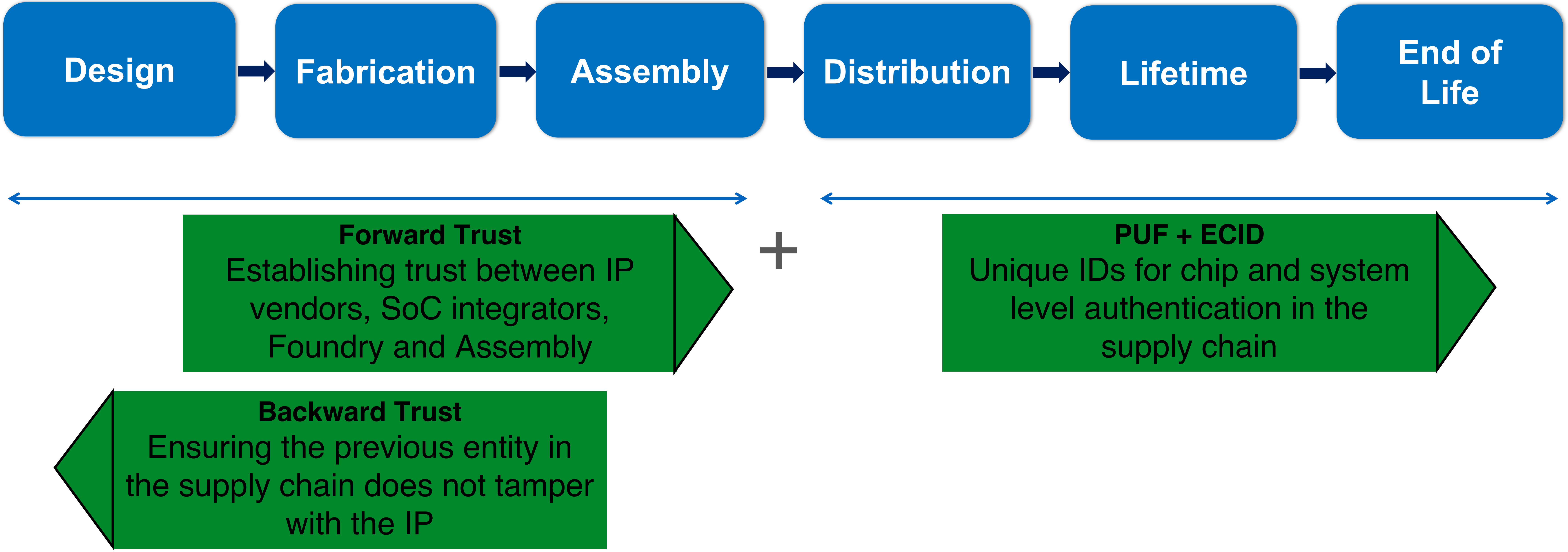
Security Goals and Attack Vectors



Goals
Attacks
Primitive / Countermeasure
Leak Sensitive Information
Modify Functionality
Reduce Reliability
Denial of Service (DOS)
Steal Design / Secrets
Identify Trade Secret
Simply Making Profit
Maliciously Circuits (Trojans)
Illegally Copy & Reproduce Designs (IP Piracy)
Reverse Engineering (RE) and Tampering
Side-Channel Attack
Counterfeiting
Trojan Detection and Prevention
Physical Unclonable Functions (PUFs)
True Random Number Generators (TRNGs)
Anti-RE and Anti-Tampering
Countermeasure for SCA
Counterfeit Detection and Anti-Counterfeiting

Protection Throughout the Lifecycle

Protection Solutions



Design → Fabrication → Assembly → Distribution → Lifetime → End of Life

Forward Trust
Establishing trust between IP vendors, SoC integrators, Foundry and Assembly

+

PUF + ECID
Unique IDs for chip and system level authentication in the supply chain

Backward Trust
Ensuring the previous entity in the supply chain does not tamper with the IP

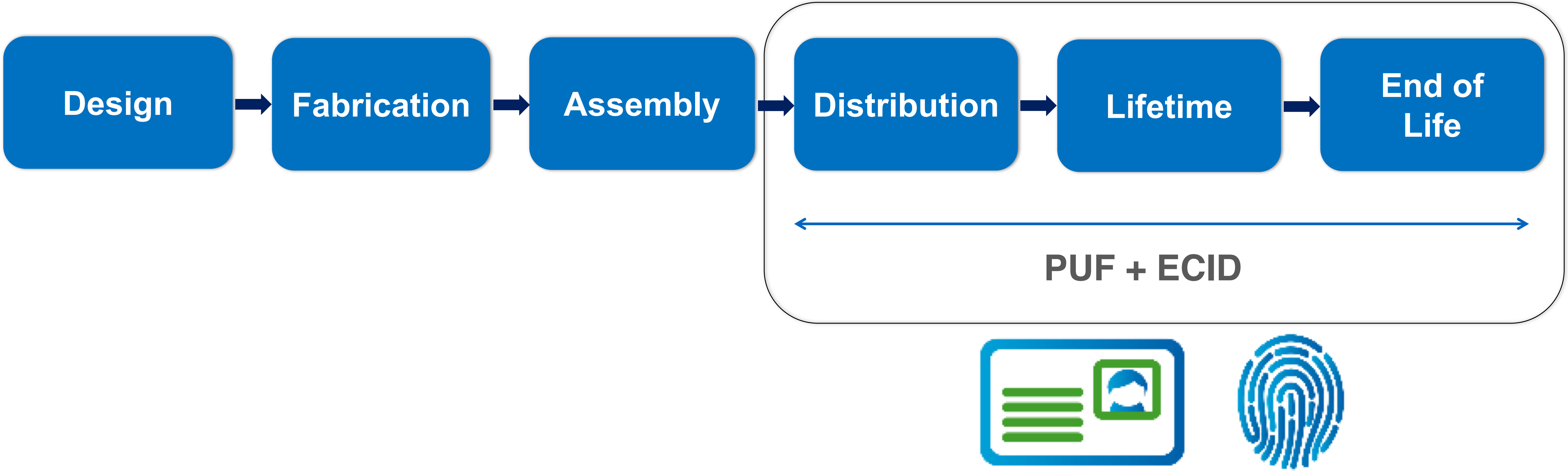
Outline

- Problem Statement and the Fundamentals
- Example Attacks
- Supply Chain Vulnerabilities
- PUF + ECID
- Counterfeit Electronics
- Logic Obfuscation / IP Encryption
- Hardware Trojans
- Research Challenges

Unique IDs

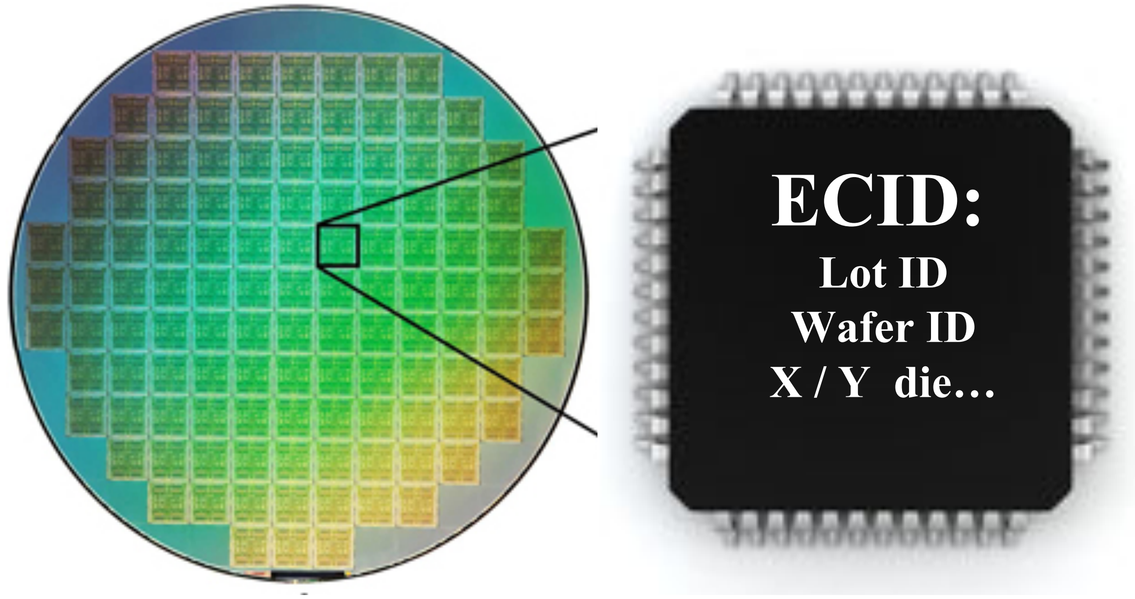
Front end of the supply chain

Back end of the supply chain



Electronic Chip ID (ECID)

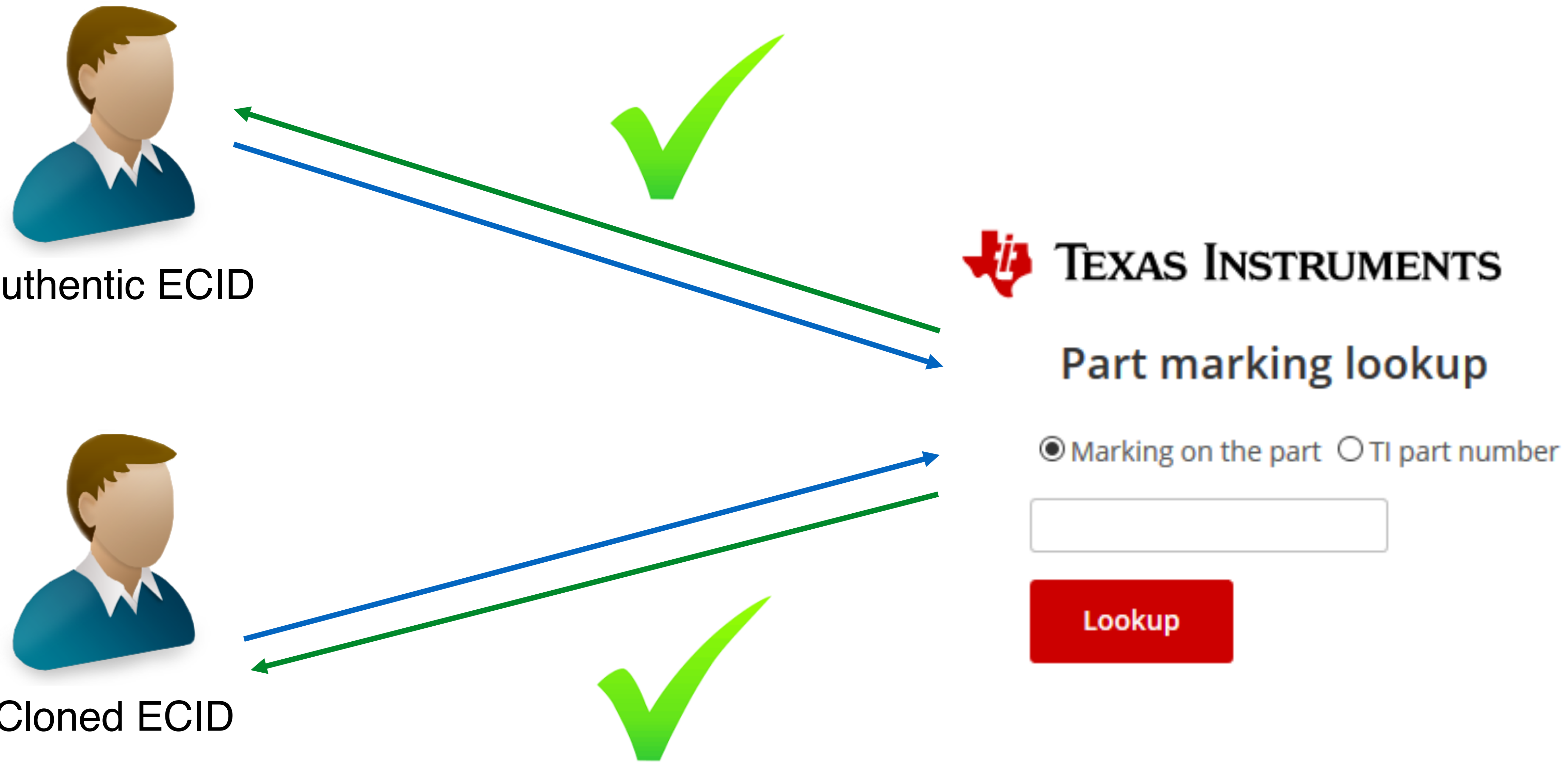
- **ECID** → Wafer X-Y locations, lot information, wafer number, **speed/temperature** grade, etc.
- **Unique** per die (ideally)
- Written in NVM, e.g., one-time programmable memory (**OTP**)



- Accessible via **JTAG**
  - IEEE 1149 → ‘ECIDCODE’ instruction to **read ECID** values
- ECID → Prevent **counterfeit,** e.g., **re-marking**
  - Retrieve **speed/temperature grade** from ECID
  - Compare with **remarked IC**

ECID Limitation

- ECID can be **cloned**
  - An attacker can retrieve **ECID** from an **authentic IC**
  - Authentic ECID → **programmed** in the OTP of the **cloned IC**



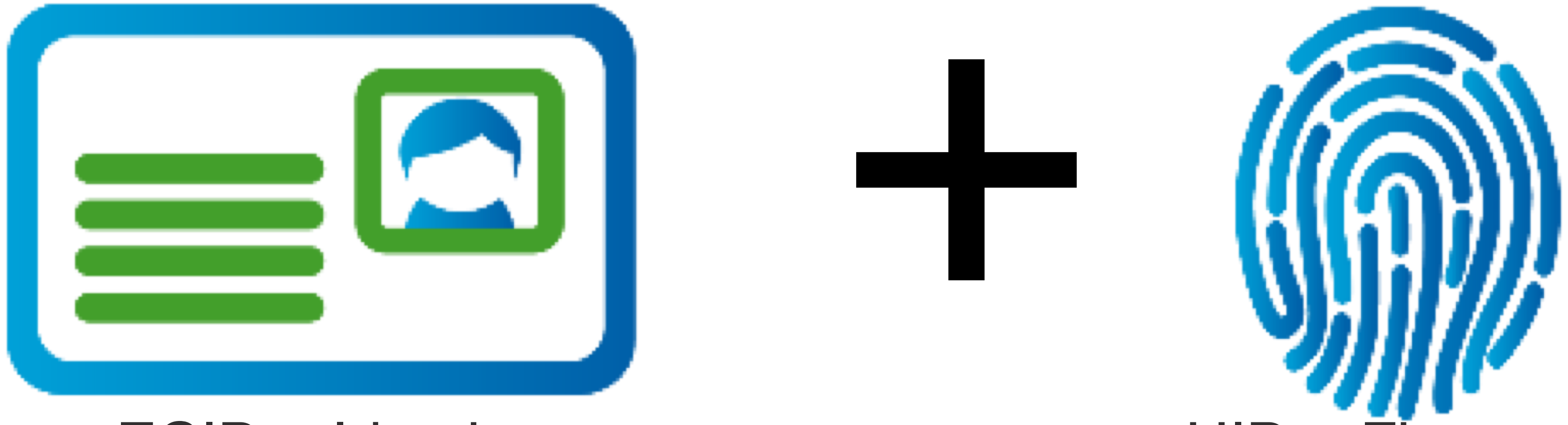
● Marking on the part ○ TI part number

Unclonable ID

- **Electronic Chip IDs (ECID)** can uniquely identify the device
- **Unclonable IDs** acting as a "**fingerprint**" – data can be read at multiple stages and provide similar results (requires fuzzy logic to compare)
- **Fingerprint Circuitry:**
  - PUFs (Physical Unclonable Functions)
  - Repeatable test data
  - SRAM startup signatures, DRAM. FLASH, etc.
- **PUFs can generate encryption keys**, enabling the chip itself to act as a "root-of-trust"

Username

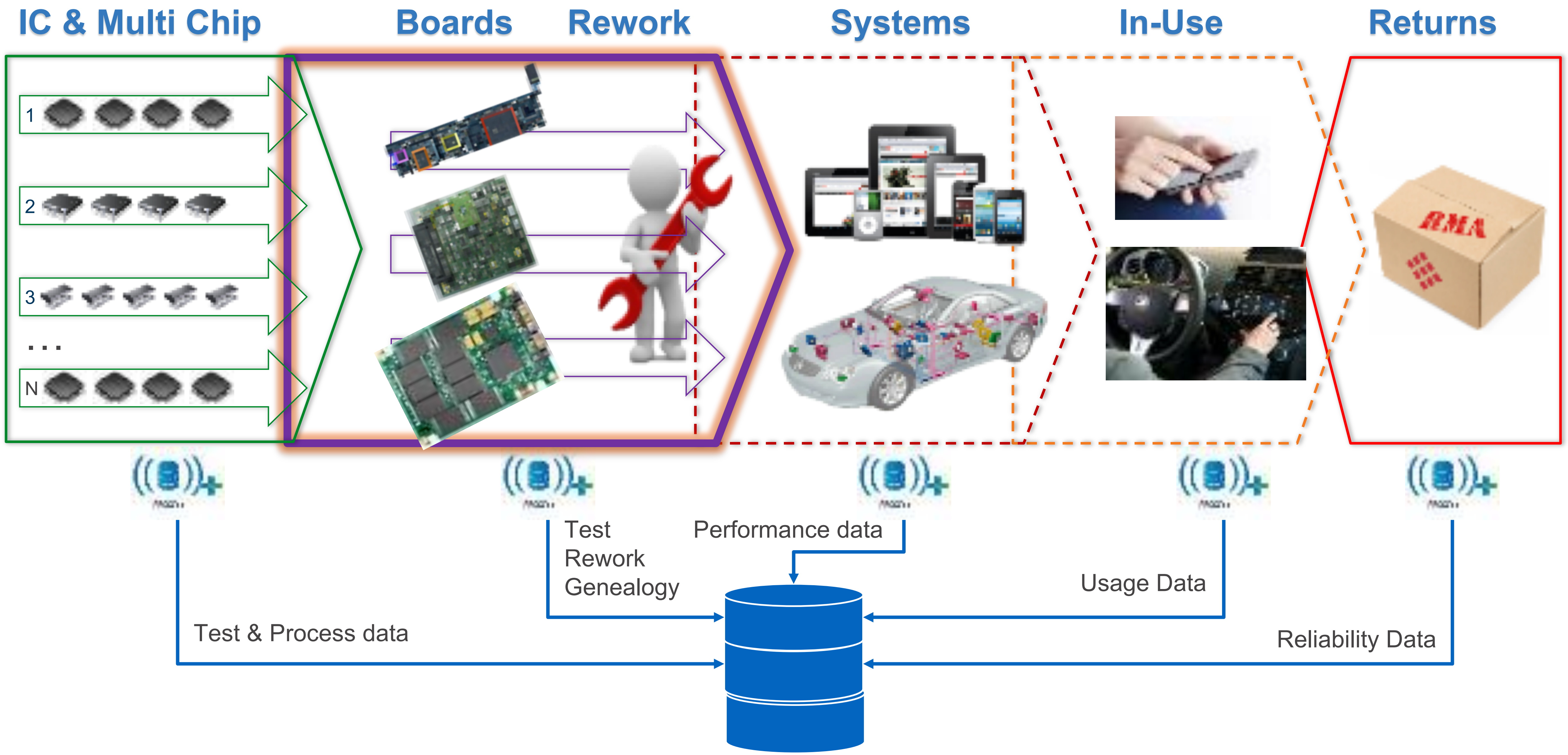
Password



ECID = Identity
(Always the same for a specific chip)

UID = Fingerprint
(Always similar for a specific chip)

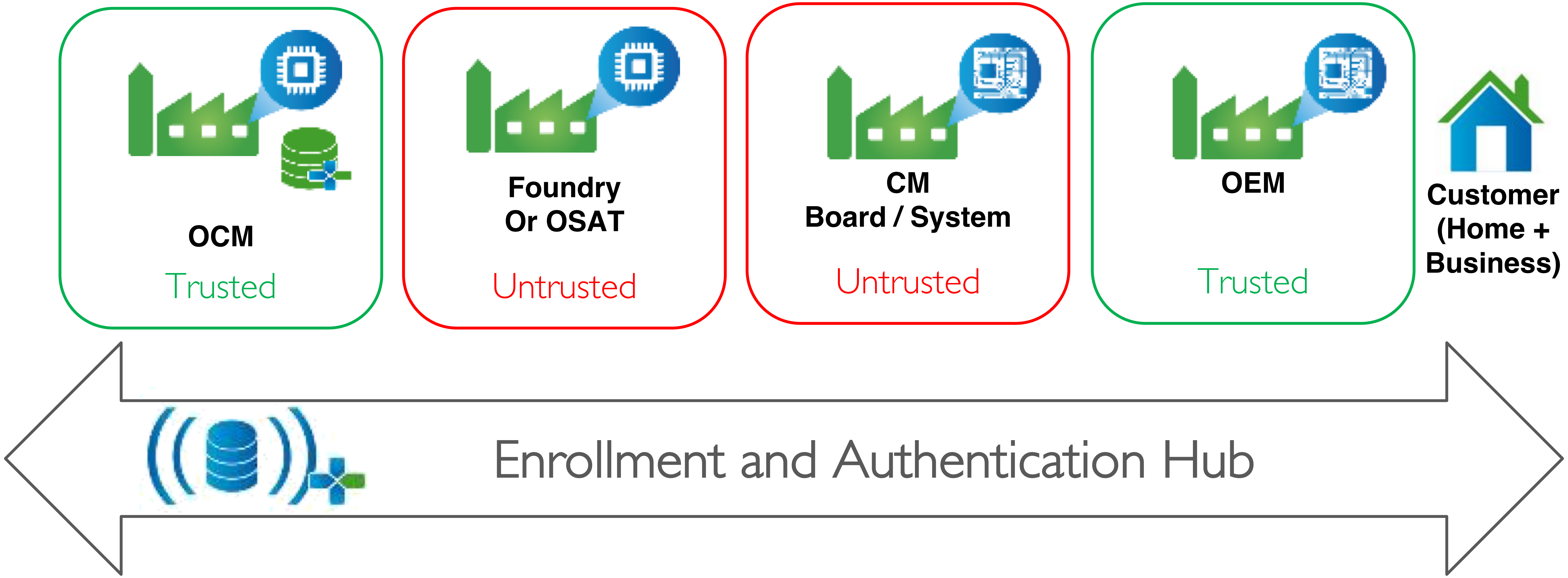
Authentication Throughout Lifecycle



Cross-industry platform connecting electronics supply chain to semiconductor identity

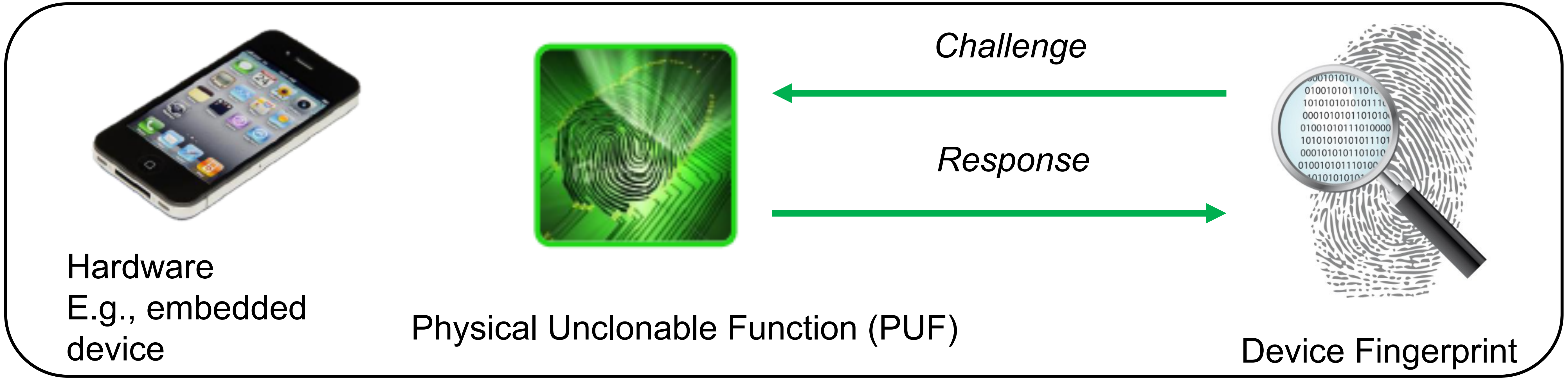
@Optimal +

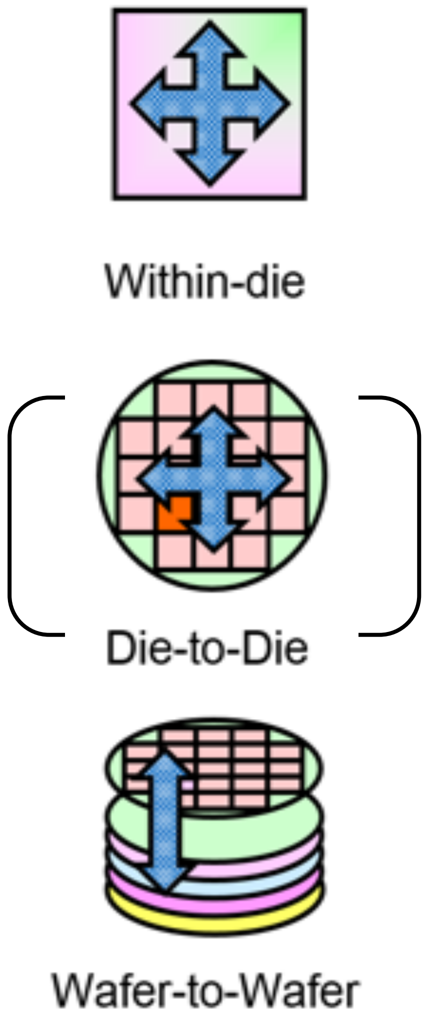
Authentication Hub

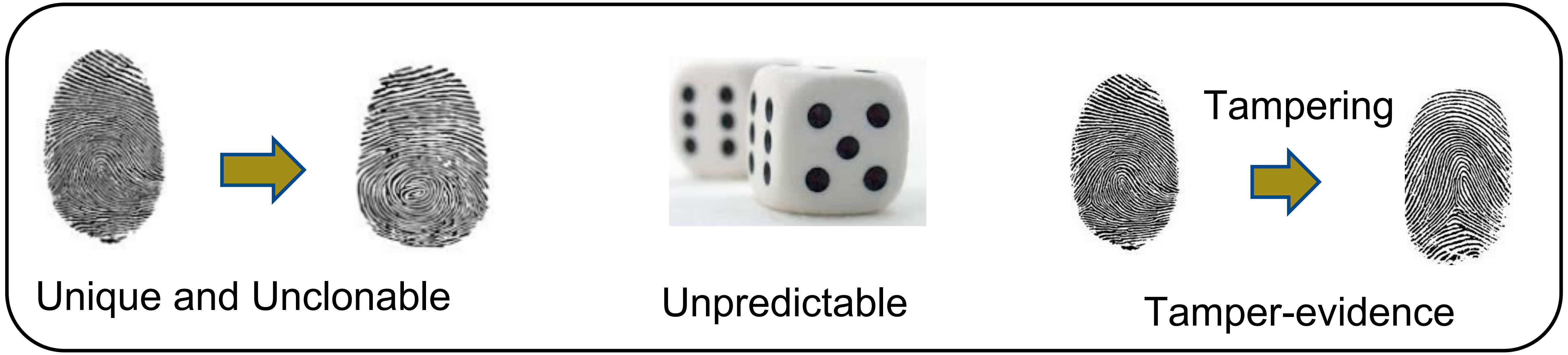


OSAT: Outsourced Assembly & Test

Physical Unclonable Functions (PUFs)



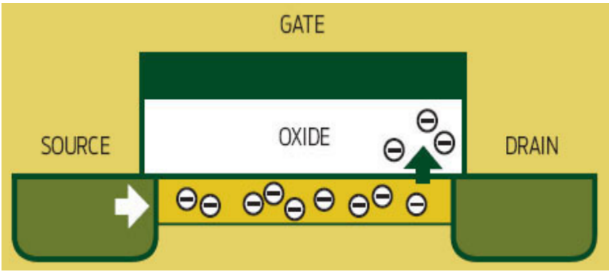




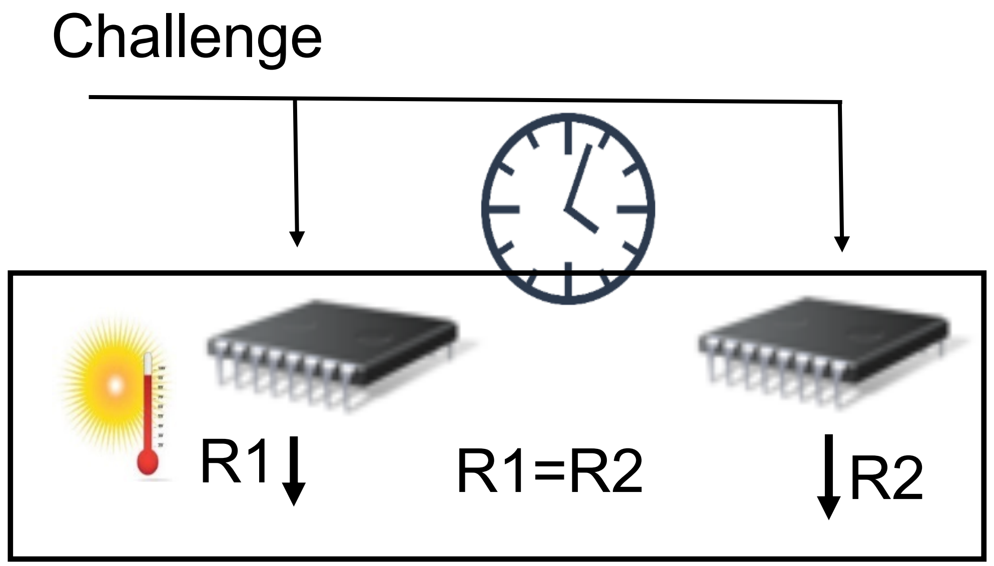
- **Uncontrollable Variations**
  - Oxide thickness
  - Device length
  - Threshold voltage (V_{th})

Quality of PUFs and Challenges

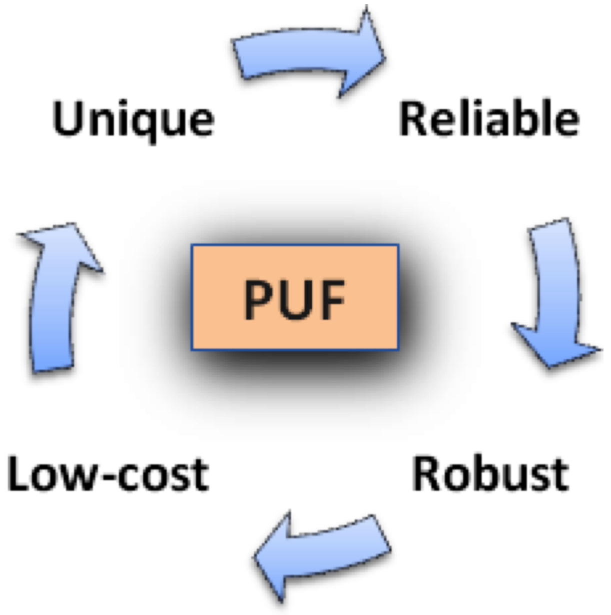
- **Major PUF Quality Metrics**
  - **Uniqueness:** systematic correlation
  - **Robustness:** aging, wear-out, environmental variations
- **Aging and wear-out**
  - **Bias Temperature Instability (BTI)**
    - Negative BTI: occurs in PMOS
    - Positive BTI: occurs in NMOS
    - Both increases transistor Vth → makes device slower
  - **Hot Carrier Injection (HCI)**
    - Increases Vth
    - Decreases mobility, reduces Ion, makes device slower
  - **Electromigration (EM)**
    - Metal ion gets displaced/removed from connections
    - Device failure, open/short connection
- **Environmental Variations**
  - **Temperature variation**
    - Thermal noise
  - **Voltage variation**

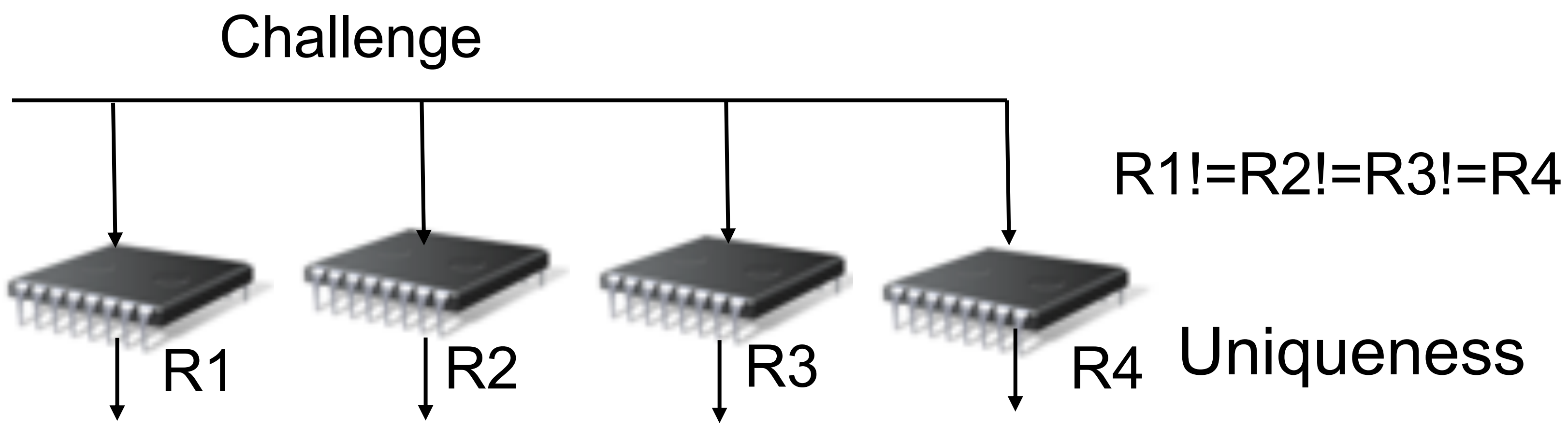


HCI



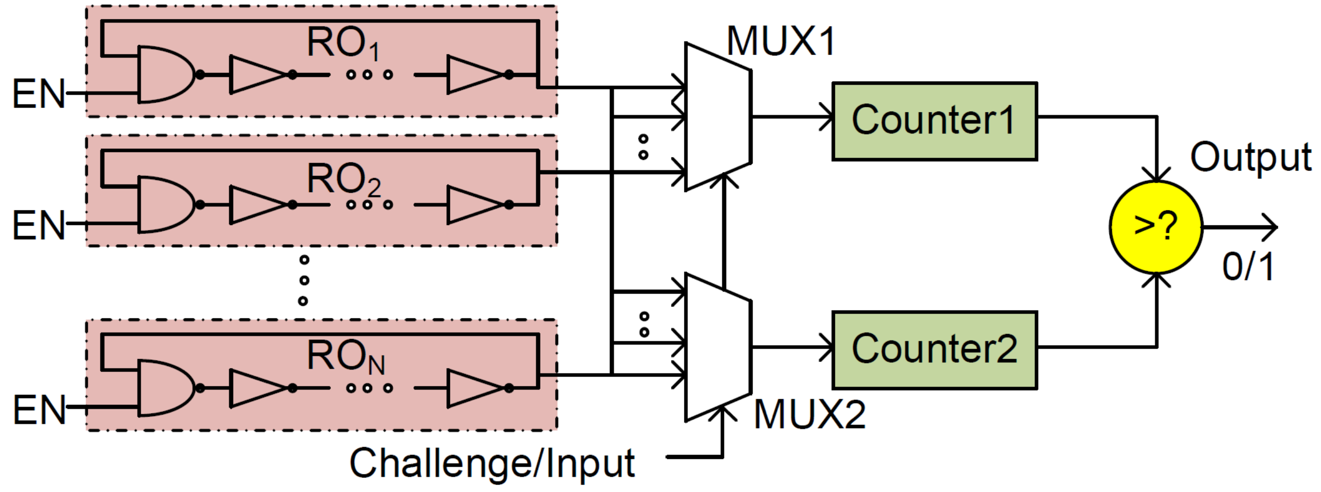
Reproducible





Uniqueness

RO-based PUF



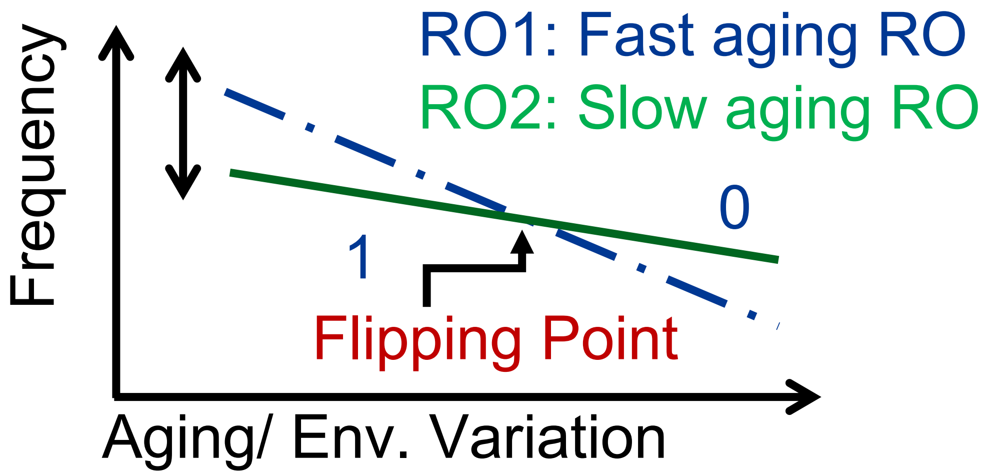
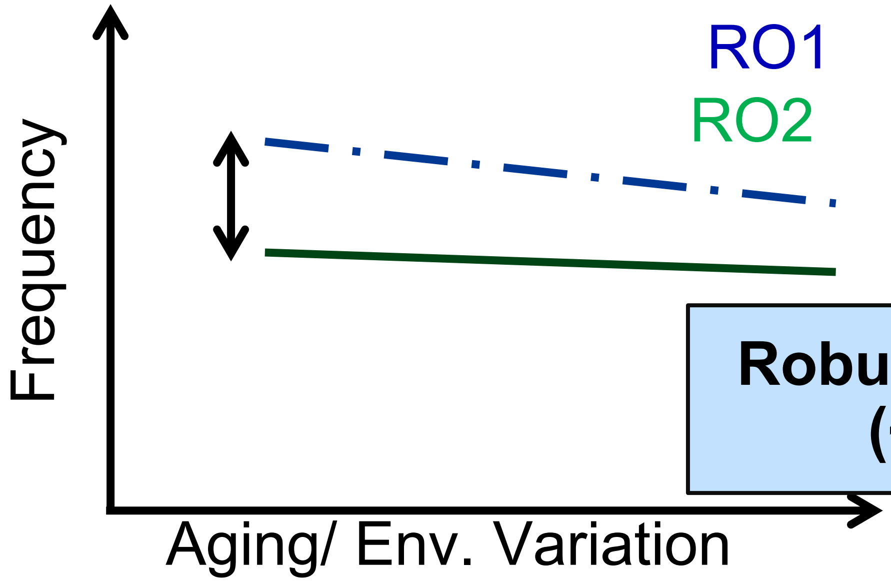


Fig: Robustness Problem

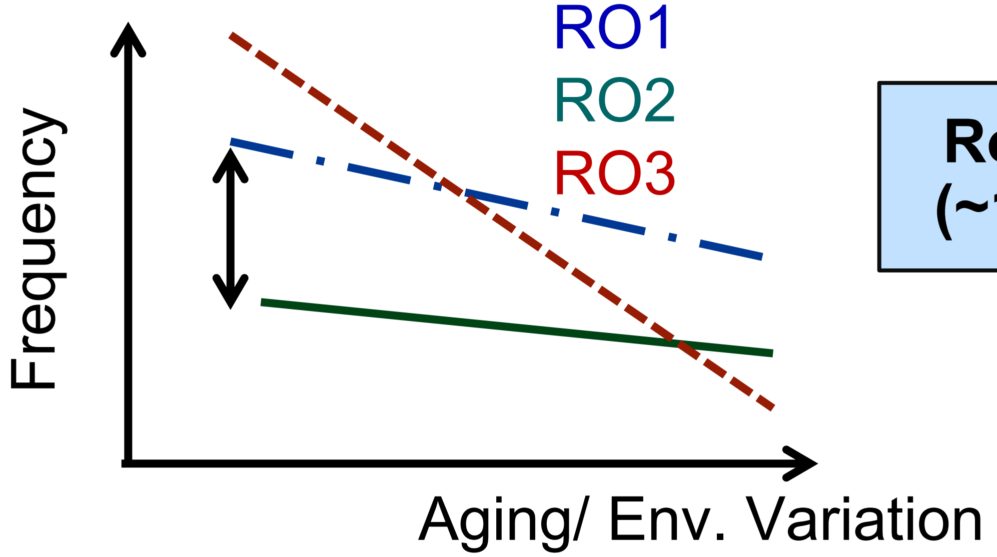
- Before Flipping Point
  - f(RO1)-f(RO2)>0==1
- After Flipping Point
  - f(RO1)-f(RO2)<0==0

Design for Robust RO-based PUF



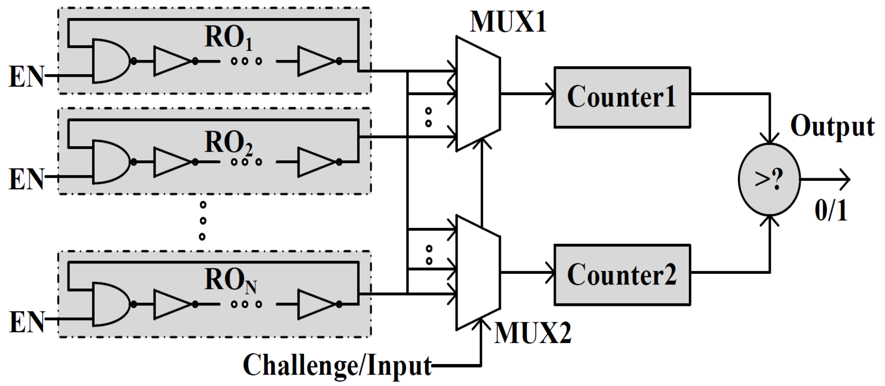
Robustness (HSPICE): ~99% (~7% improvement)

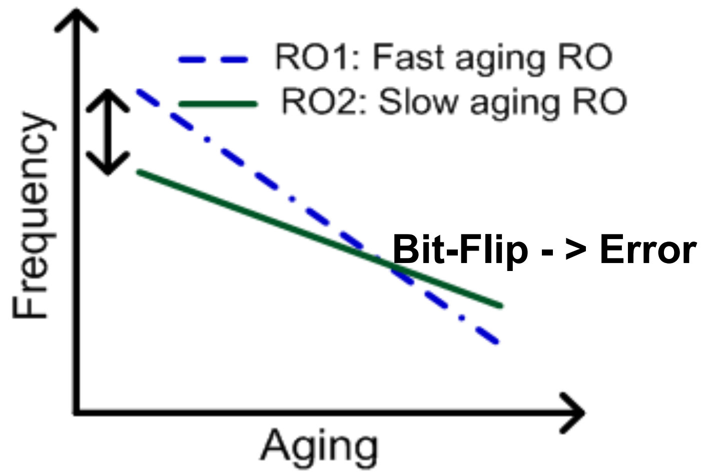
RePa: Reliable pair selection algo.

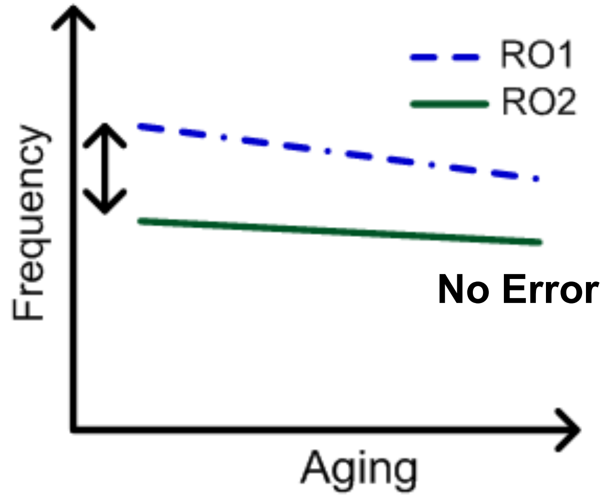


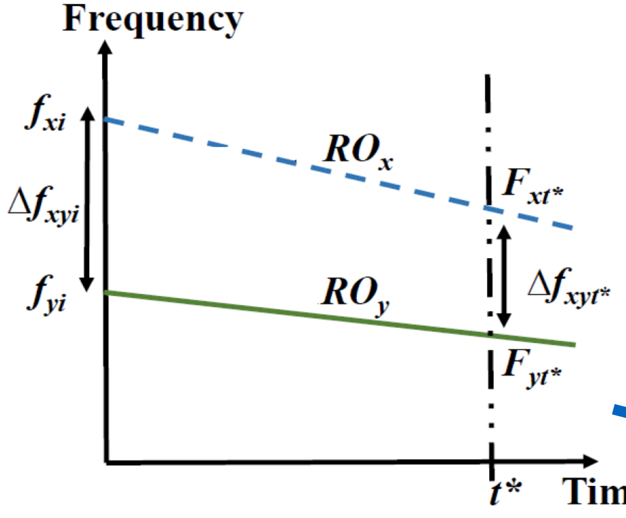
Robustness: ~100% (~11% improvement)

Reliable RO Pair Formation (RePa) Scheme









ROs with negligible degradation (Highly Stable pair)

RePA Key Strategy

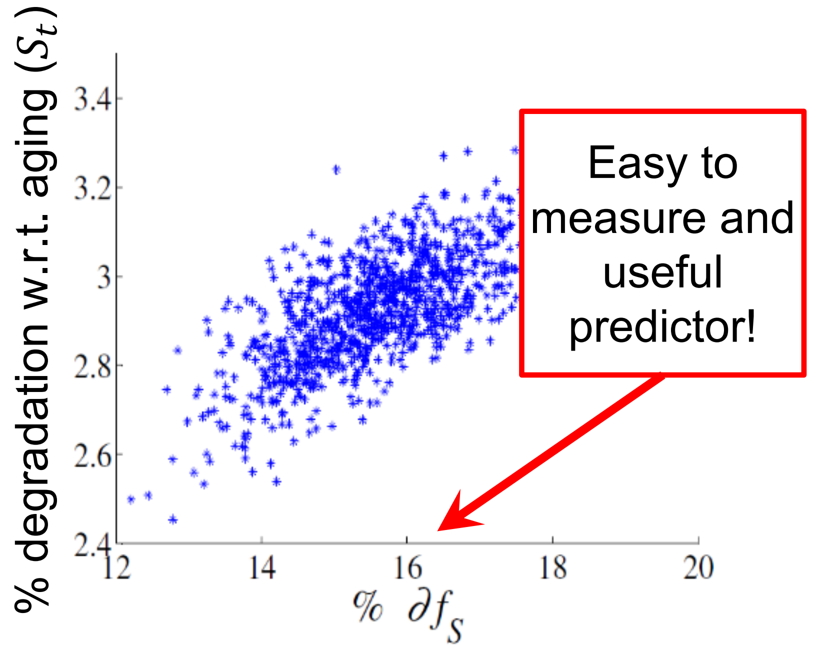
Select ROs with minimal crossover possibilities for intelligent pair formation.

RePa sorts and selects ROs into pairs such that

$$\Delta f_{xy_{inital}} \rightarrow \text{High}; \Delta S_{xy} \rightarrow \text{Low}$$

$$\Rightarrow \Delta f_{xy_{inital}} > \Delta S_{xy}\ t^*\text{: True for all } t^*$$

- **Key Question:** How does one estimate $S_x$and S_y?
- **RePa** scheme uses correlation of aging degradation and degradation due to Vdd variation!
  - Aging prediction
    - Burn-in test → costly and time consuming.
    - Electrical Test (using correlation) → Low cost and fast
- RePa can achieve 100% reliability eliminating the need for ECC

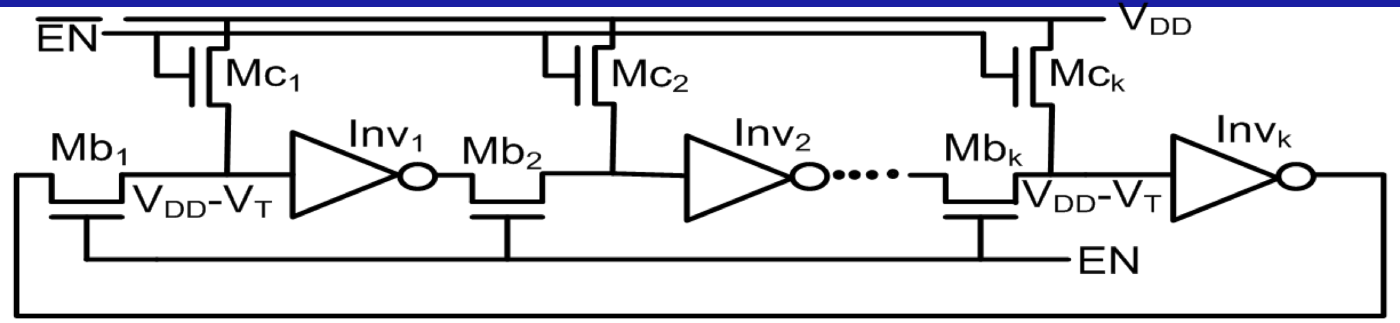


Easy to measure and useful predictor!

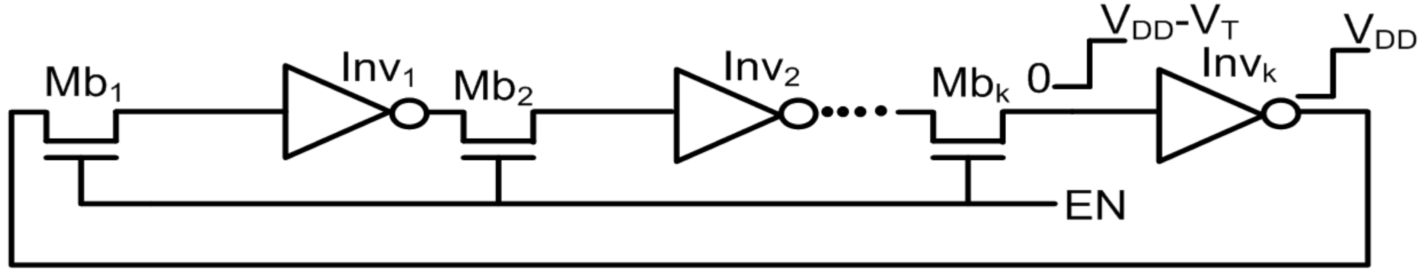
% degradation w.r.t. Vdd (S_v)

ARO-PUF

Overall ARO-PUF Design



ARO-PUF in Oscillatory Mode



ARO-PUF in Non-oscillatory mode

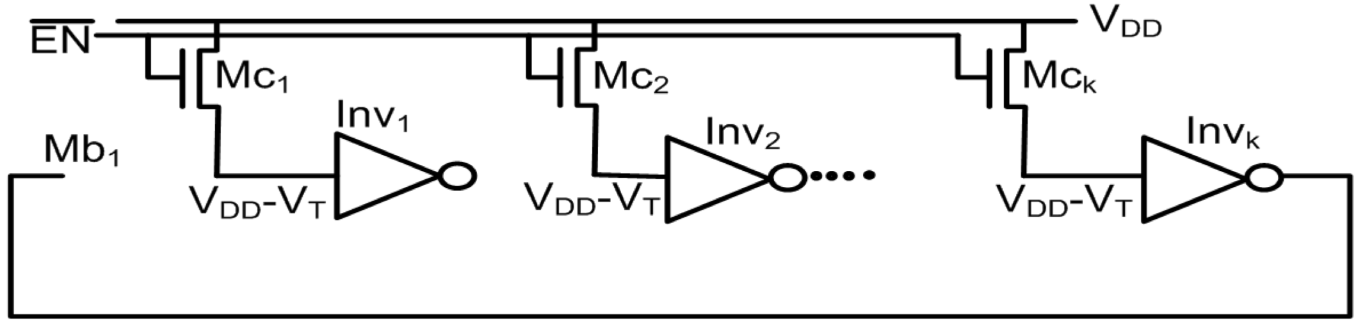
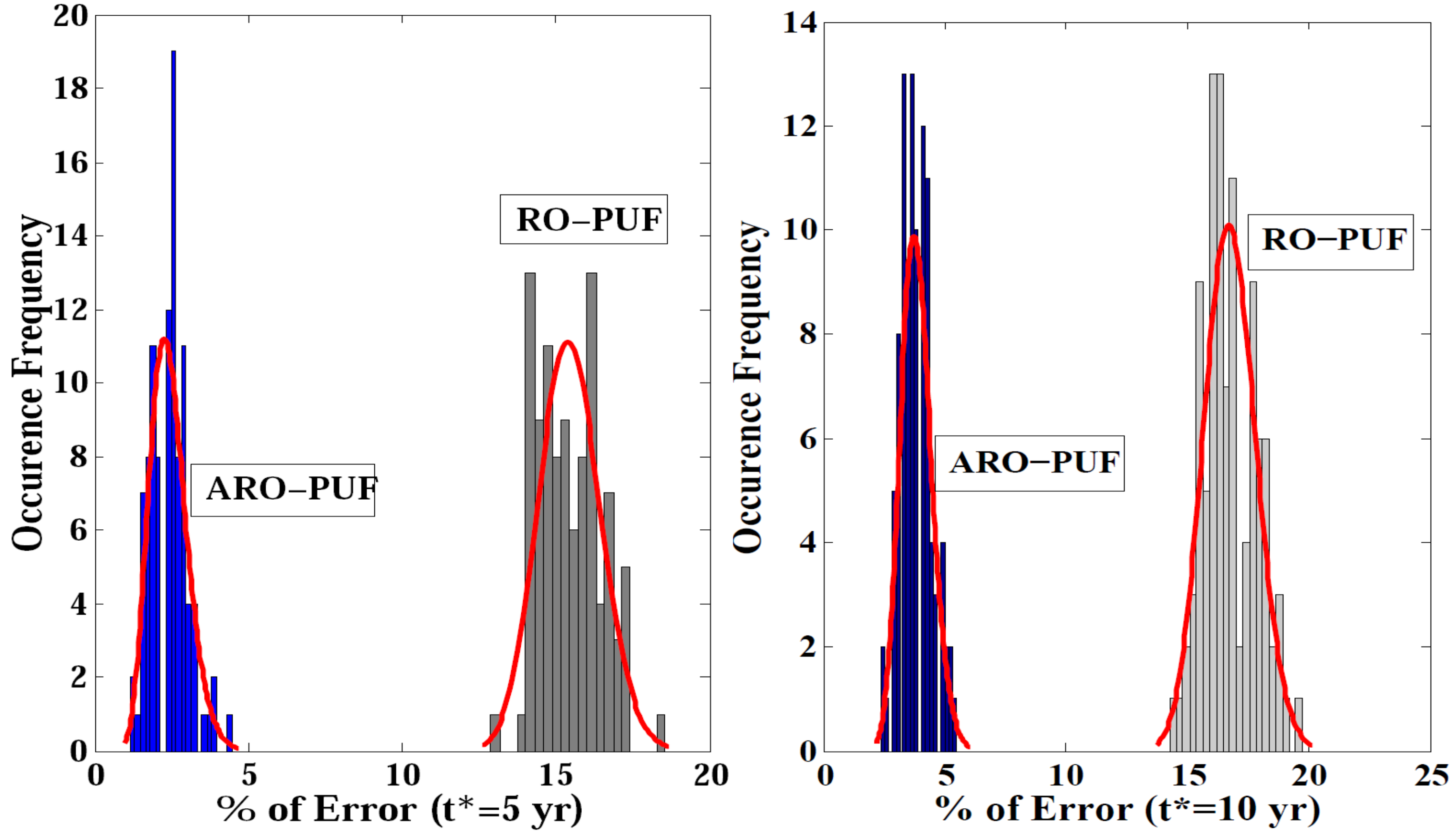
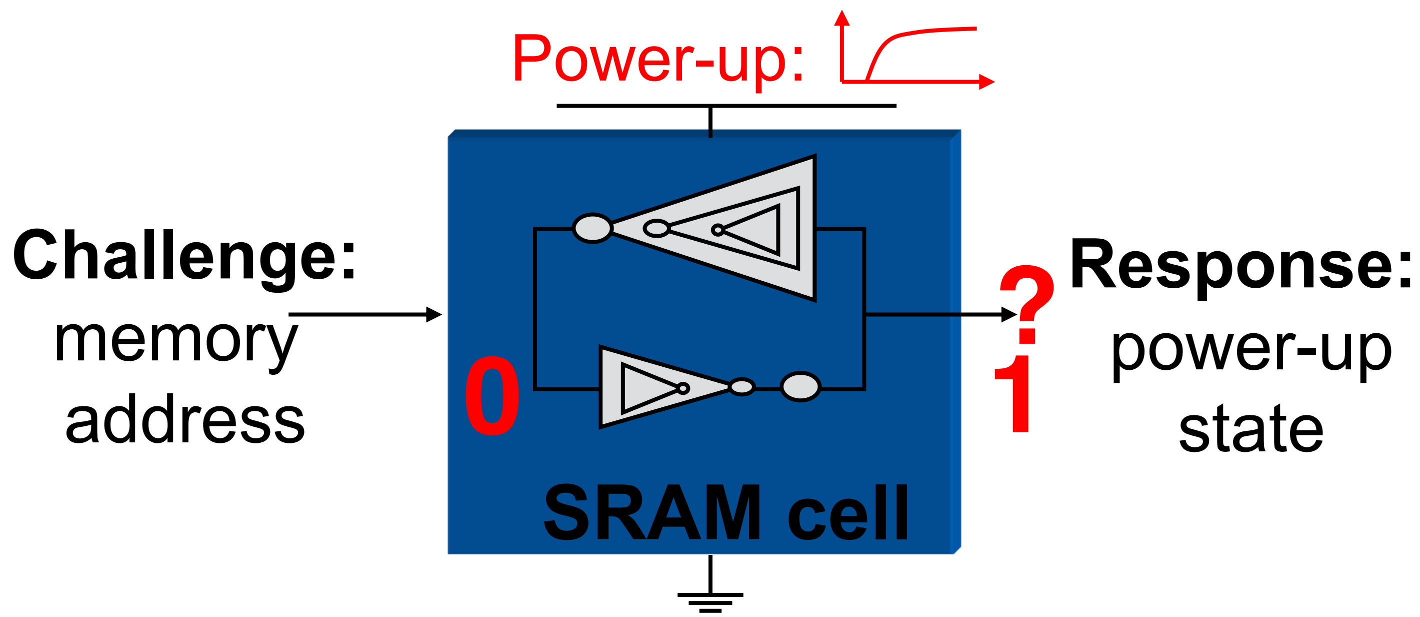


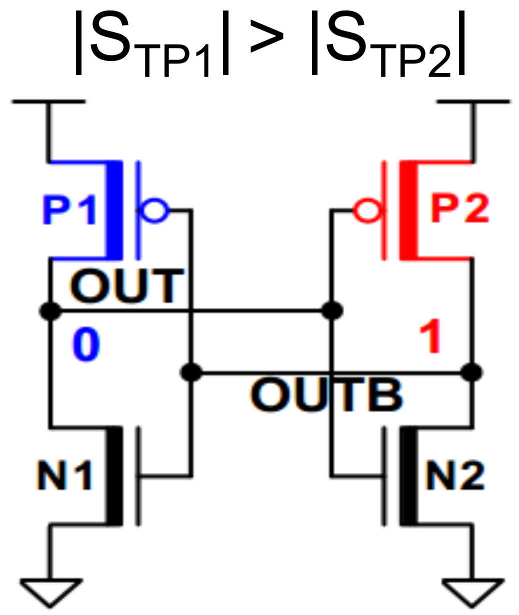
Table 3: Aging Degradation		
Active-ation Time	ARO-PUF	
	Freq. Degrad-ation	Avg. Error
5%	1.54%	1.98%
1%	1.34%	1.45%

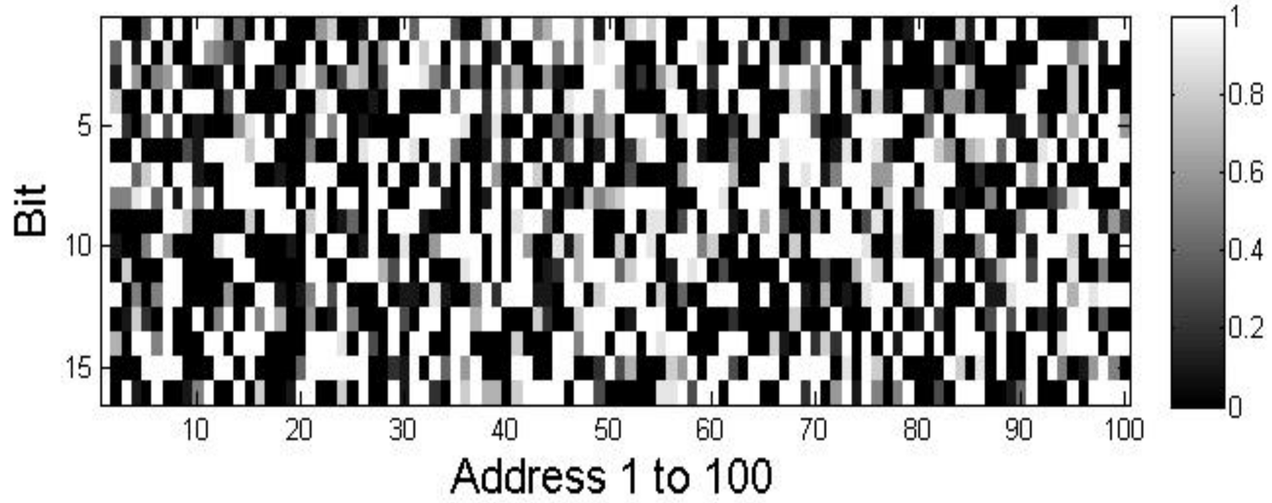
Aging Error		
Use	Avg. Error	
	ARO- PUF	RO-PUF
5 yrs	2.43%	11.46%
10 yrs	3.83%	12.76%

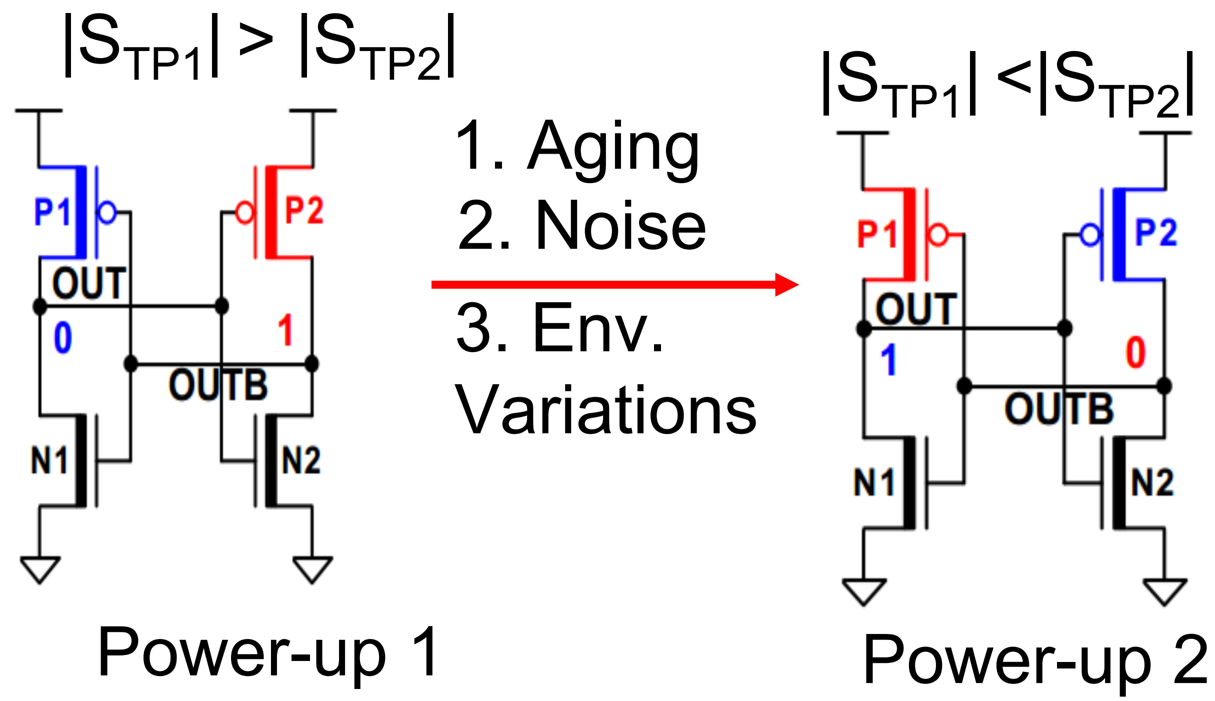


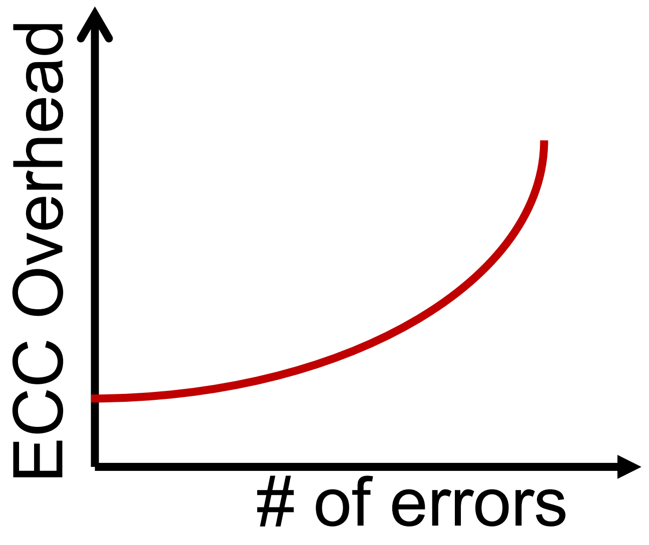
SRAM-based PUF and Challenges









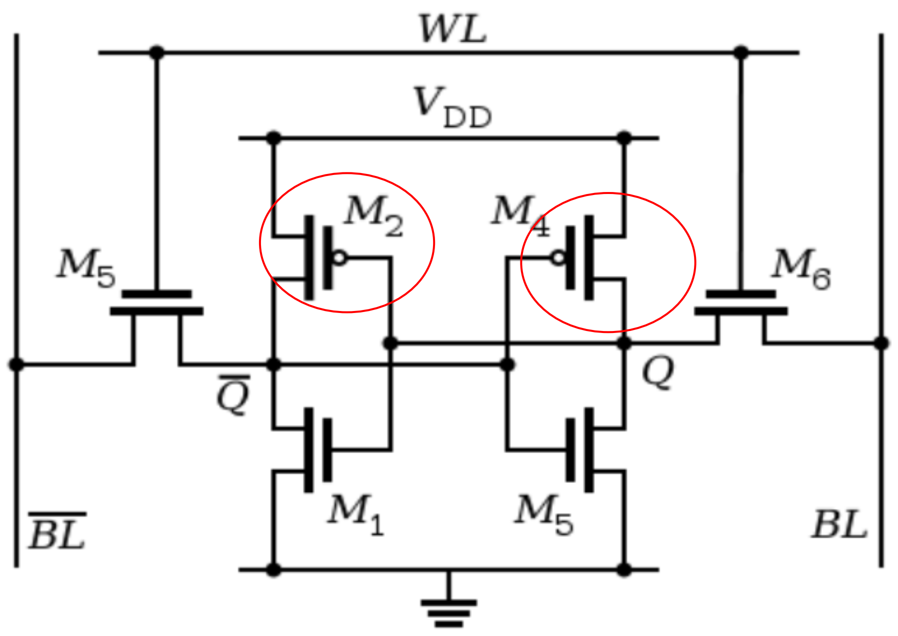


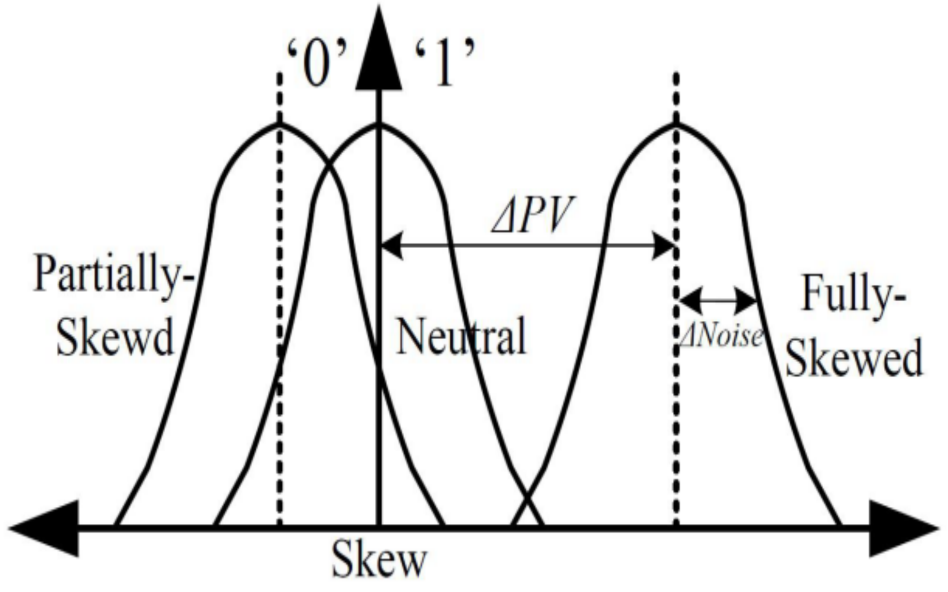
- **ECC:** Area and power overhead
- **Objective:** selecting SRAM cells for robust key generation
- Neighborhood-based cell selection approach
  - Noise Sensitivity: Neighborhood-based Noise Interference
  - Strong (noisy) neighbors make a weak cell strong (noisy)
- Physical layout is not revealed by SRAM vendors

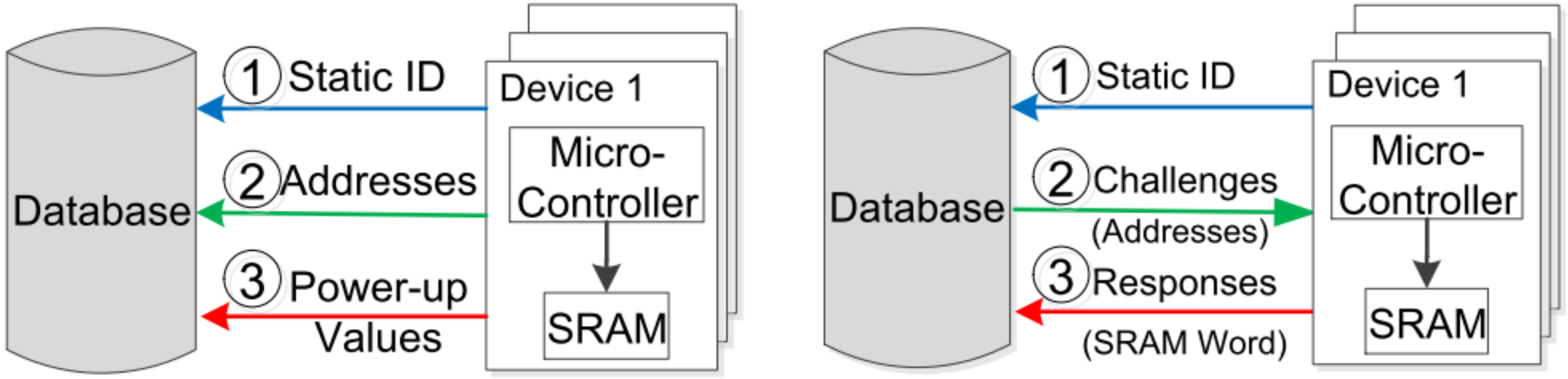
SRAM Physical Unclonable Function (PUF)

SRAM-PUF:

- SRAM is based on a bi-stable latch which will retain its values as long as the circuit is powered.
- A mismatch between the inverter pairs affecting their power-up states.
- It maps a challenge to a response.

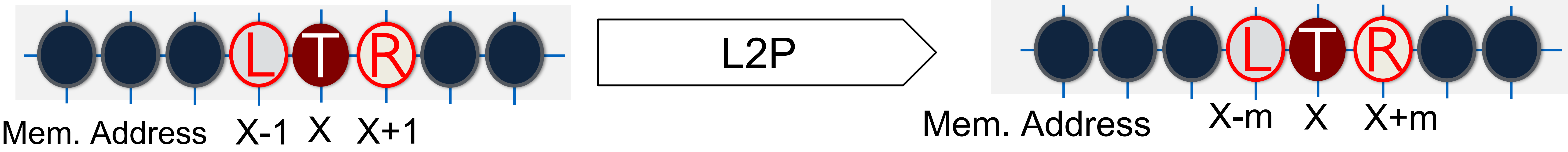






Memory PUF

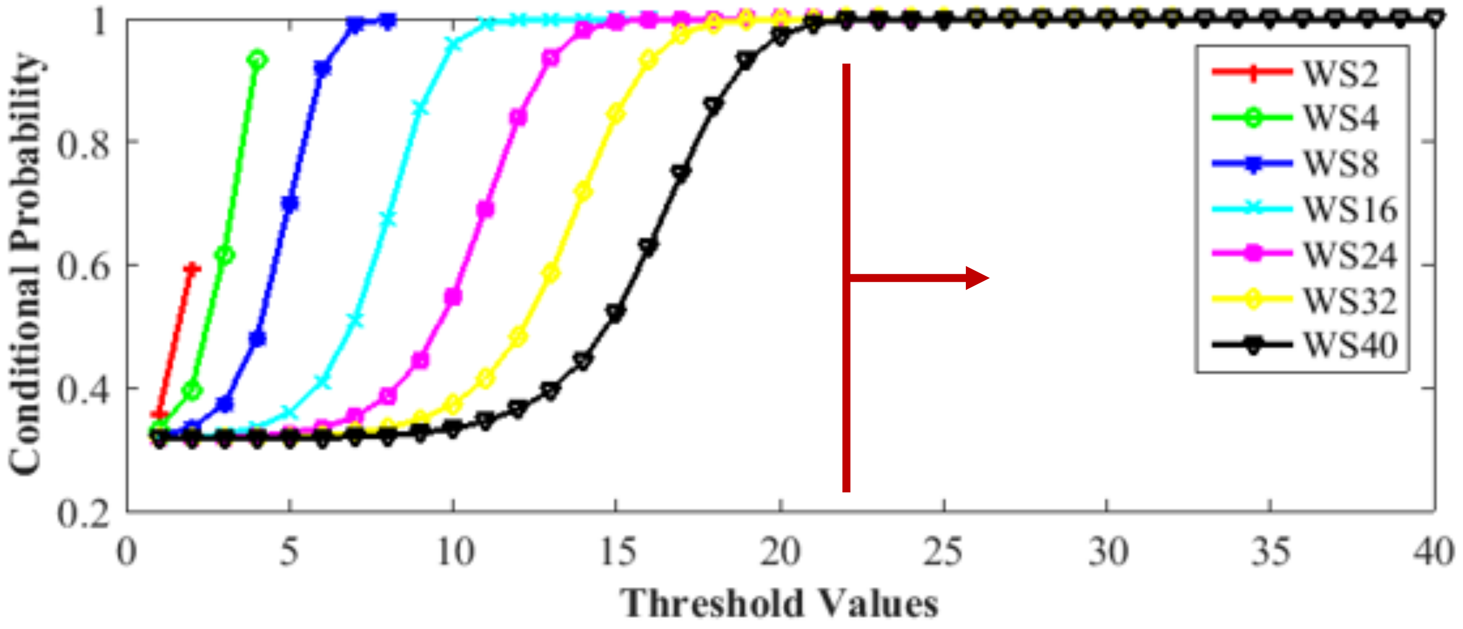
SRAM-PUF: Neighborhood-based Algorithm



Logically adjacent

Physically adjacent

Threshold= number of stable cells in a window



Cell Selection Algo.	Bit Error Rate	Uniqueness
Neighborhhod-based Algorithm	6.1e-6 (639X)	48.35%
Random	3.9e-3	48.12%

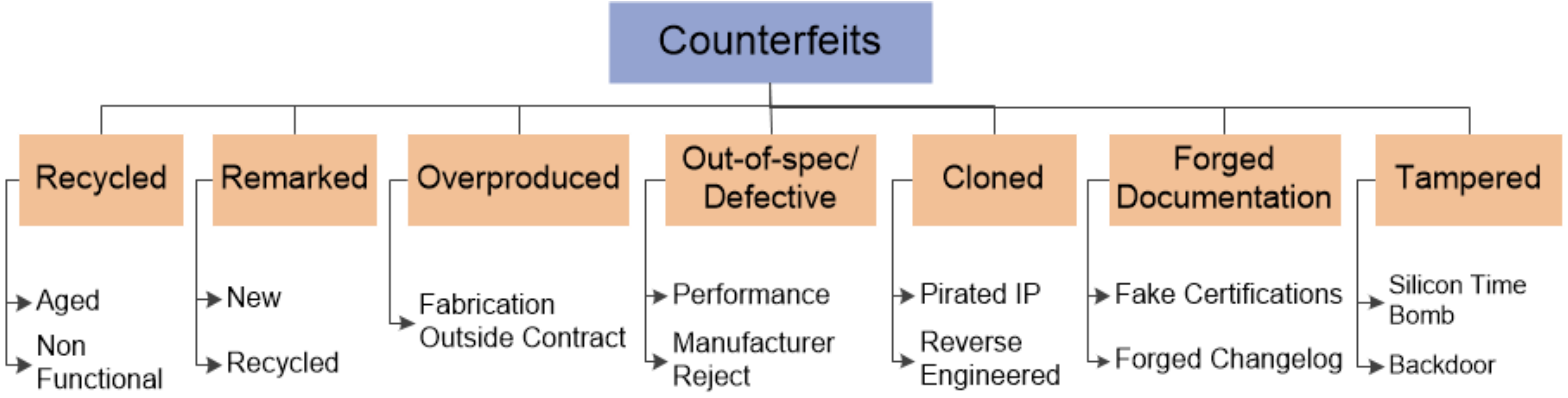
Best Candidates: cells that have 22 physically adjacent (neighbor) cells

Requires ~2.2X cells (~220 cells to generate a100-bit key)

Outline

- Problem Statement and the Fundamentals
- Example Attacks
- Supply Chain Vulnerabilities
- PUF + ECID
- Counterfeit Electronics
- Logic Obfuscation / IP Encryption
- Hardware Trojans
- Research Challenges

Counterfeit Incidents



Counterfeits

Recycled
- Aged
- Non Functional

Remarked
- New
- Recycled

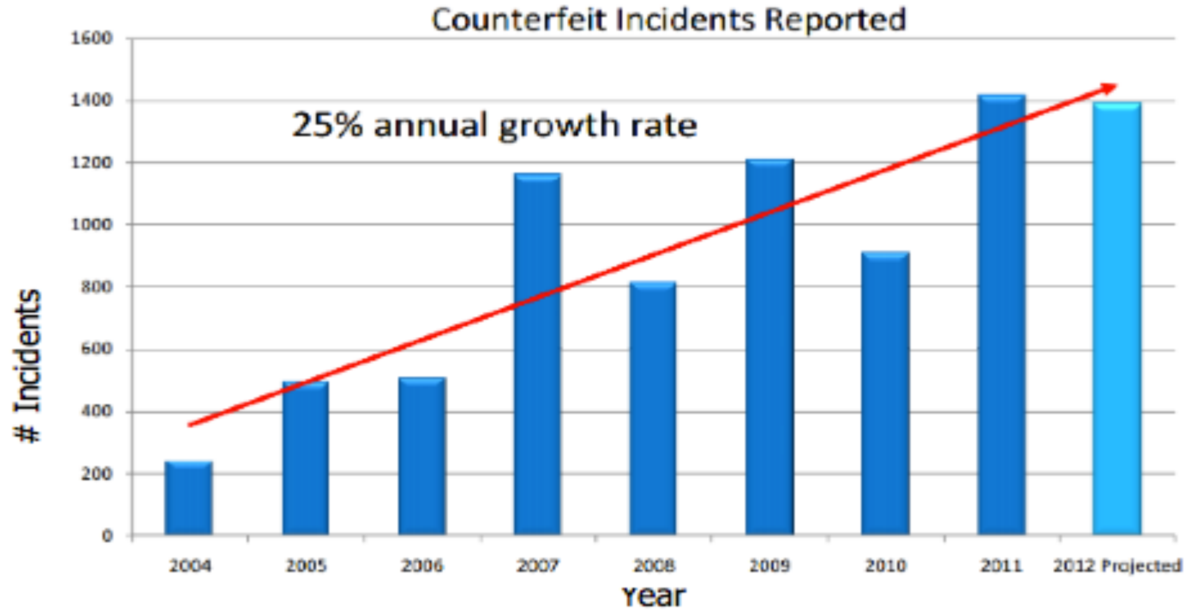
Overproduced
- Fabrication Outside Contract

Out-of-spec/ Defective
- Performance
- Manufacturer Reject

Cloned
- Pirated IP
- Reverse Engineered

Forged Documentation
- Fake Certifications
- Forged Changelog

Tampered
- Silicon Time Bomb
- Backdoor

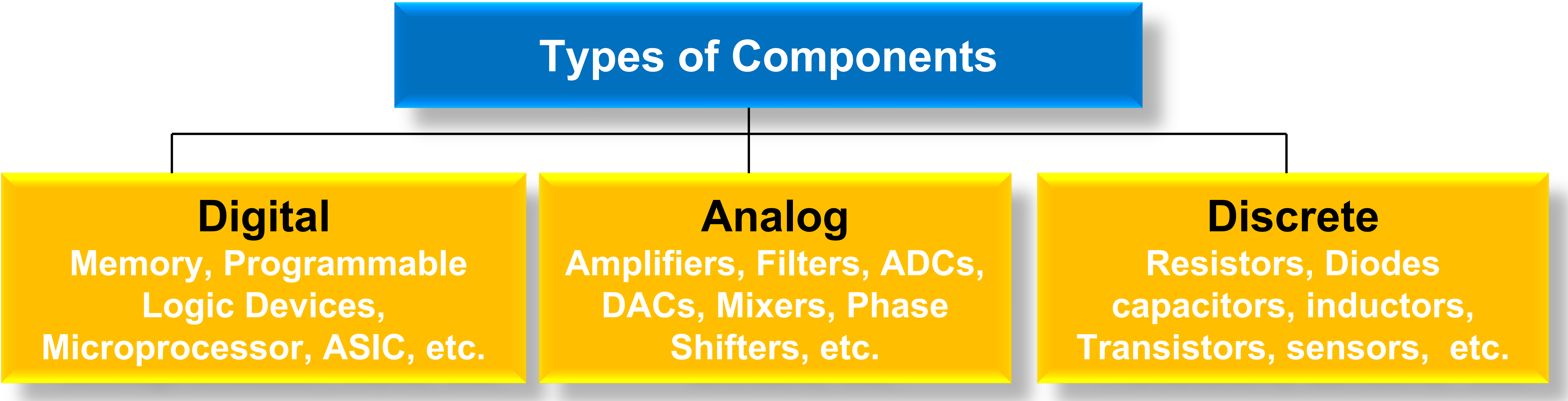


Reported counterfeit incidents are growing rapidly since 2009.

Electronics companies loses $100 billion dollar every year because of counterfeiting

U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead," Journal of Electronic Testing: Theory and Applications (JETTA), 2014.

Components

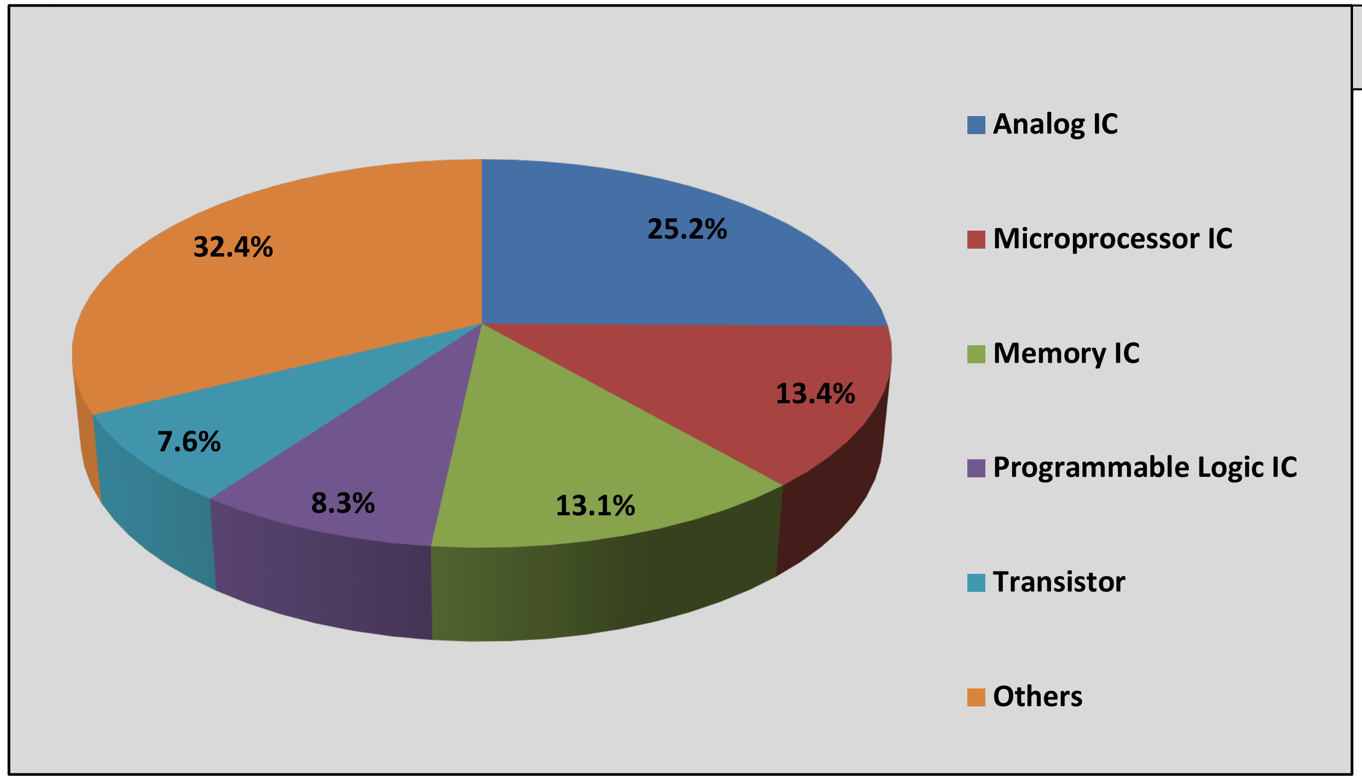


Types of Components

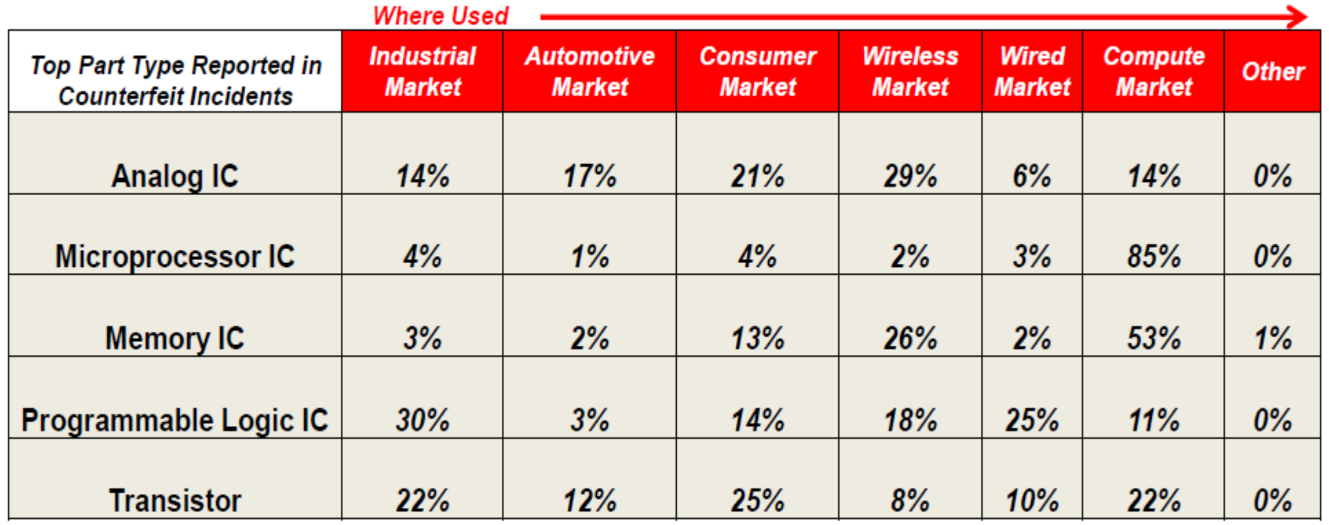
Digital
Memory, Programmable Logic Devices, Microprocessor, ASIC, etc.

Analog
Amplifiers, Filters, ADCs, DACs, Mixers, Phase Shifters, etc.

Discrete
Resistors, Diodes capacitors, inductors, Transistors, sensors, etc.



IHS reports a $169B annual risk



Where Used →

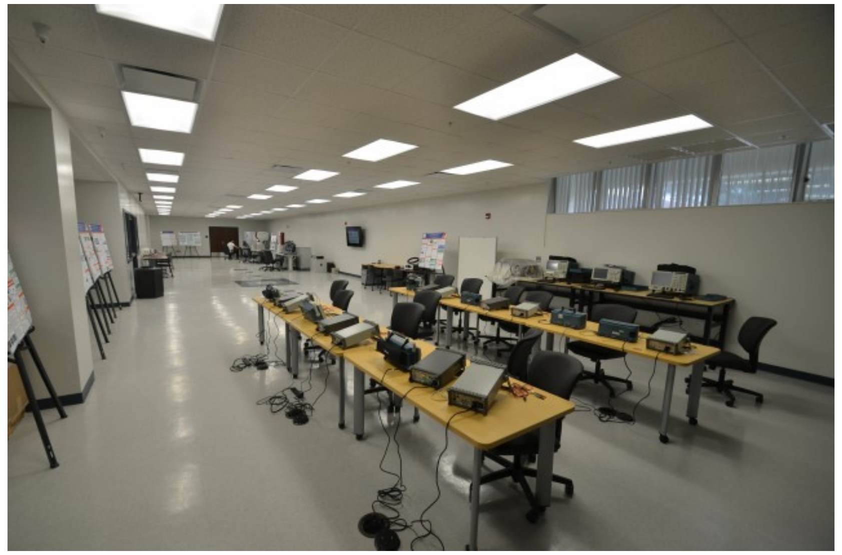
Top Part Type Reported in Counterfeit Incidents	*Industrial Market*	*Automotive Market*	*Consumer Market*	*Wireless Market*	*Wired Market*	*Compute Market*	*Other*
Analog IC	*14%*	*17%*	*21%*	*29%*	*6%*	*14%*	*0%*
Microprocessor IC	*4%*	*1%*	*4%*	*2%*	*3%*	*85%*	*0%*
Memory IC	*3%*	*2%*	*13%*	*26%*	*2%*	*53%*	*1%*
Programmable Logic IC	*30%*	*3%*	*14%*	*18%*	*25%*	*11%*	*0%*
Transistor	*22%*	*12%*	*25%*	*8%*	*10%*	*22%*	*0%*

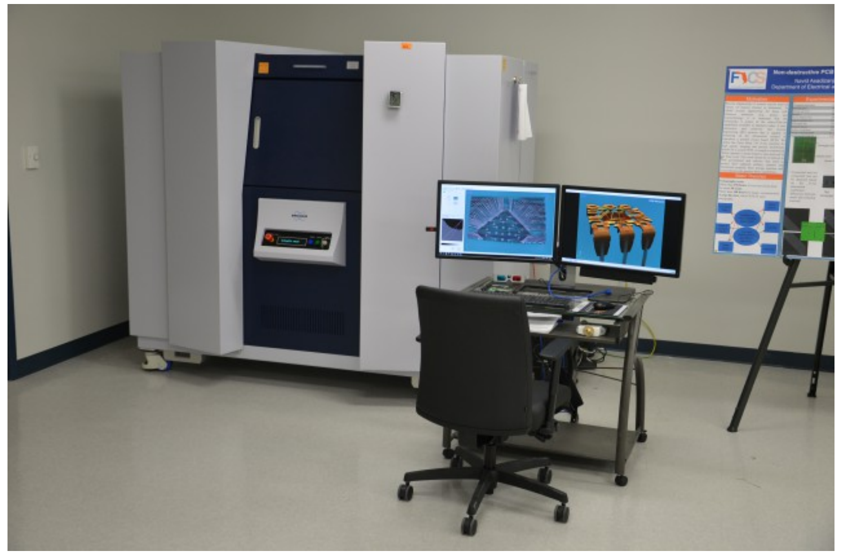
The top five represent $169 billion of semiconductor revenue in 2011, according to IHS iSuppli Application Market Forecast Tool (AMFT)

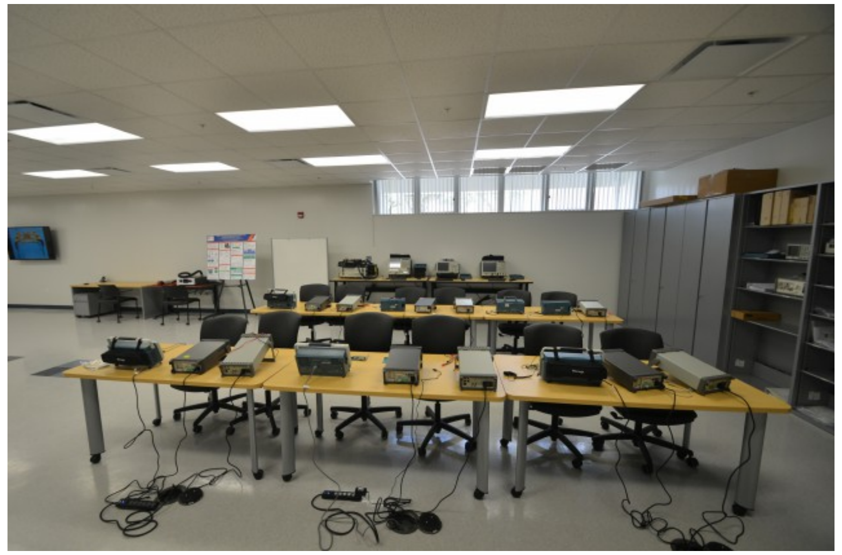
Anti-Counterfeit Mechanisms

		Recycled (Used)	Remarked (Used)	Remarked (New)	Overproduced (New)	Out-of-Spec/ Defective (New)	Cloned
Digital & Small		CDIR Structures (Fuse/ Contact)		ECID Nano Particles			Nano Particles
Transistors, Diodes, and Passive Parts		Nano Particles					
Digital & Large	Programmable Logic ICs	CDIR Structures (RO-Based, CAF-Based, SAF-Based, Fuse/Contact-Based), Nano Particles		SST, ECID	SST	SST	SST, Nano Particles
	Memory ICs						
	Microprocessor ICs						
Analog & Mixed Signal ICs		CDIR Structures (Fuse/ Contact Based)					Nano Particles

SCAN Lab, FICS Institute







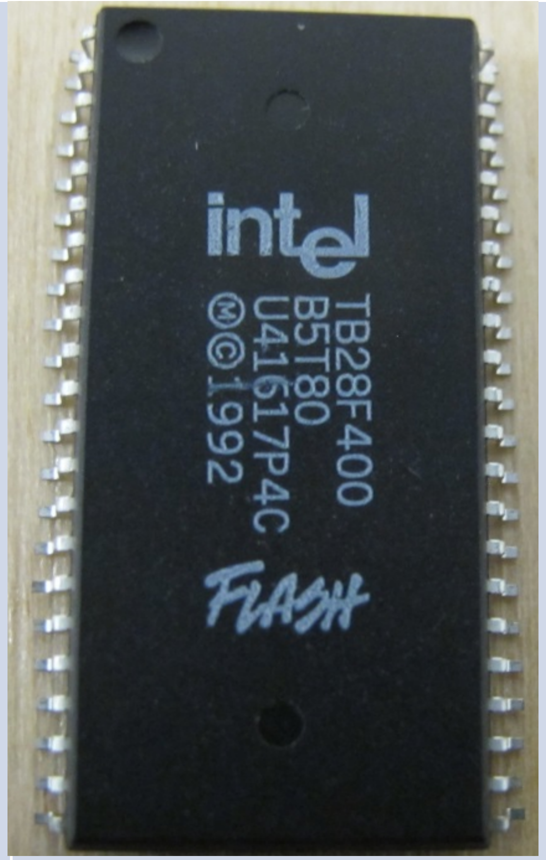
http://fics-institute.org/ http://fics-institute.org/facilities/

SCAN Lab

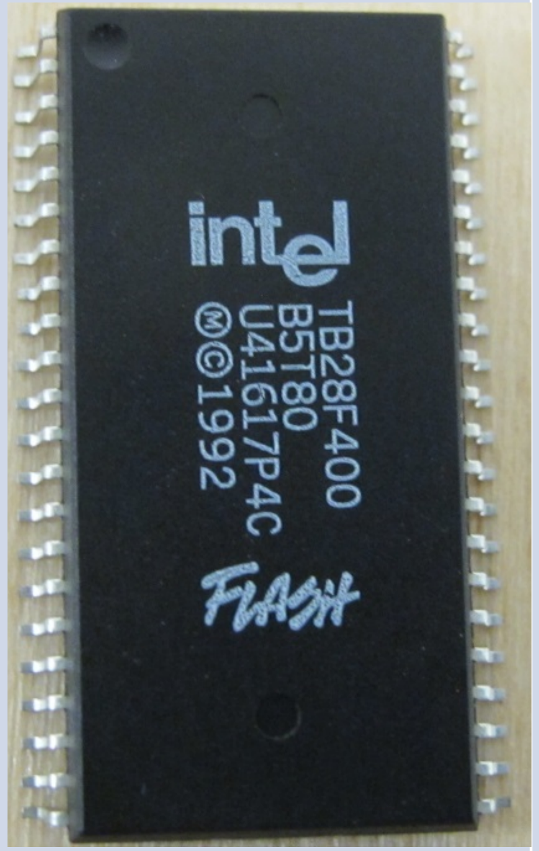
Visual Inspection

Sample 1

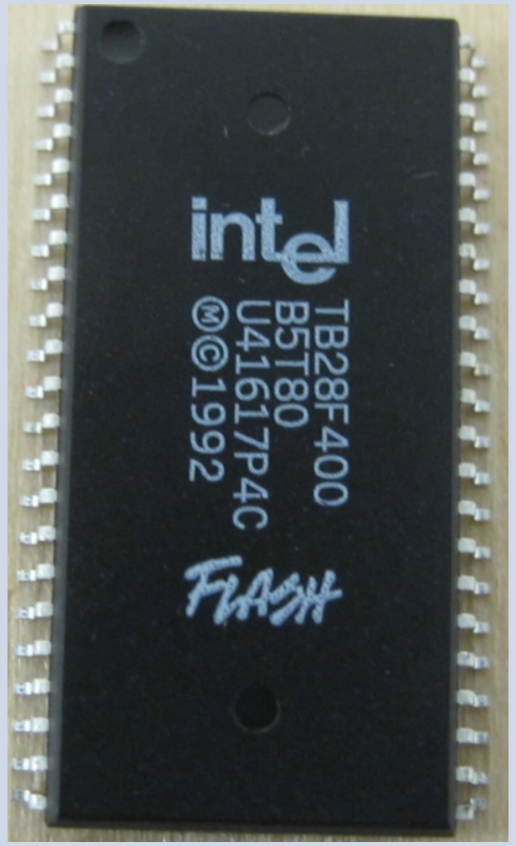
Sample 2



Sample 3



Sample 4



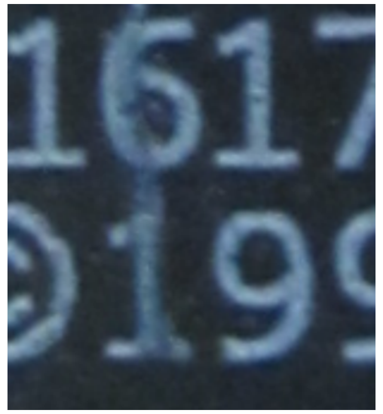
Sample 5

Same Lot Codes Same Appearance: No visible discrepancy

Observations:

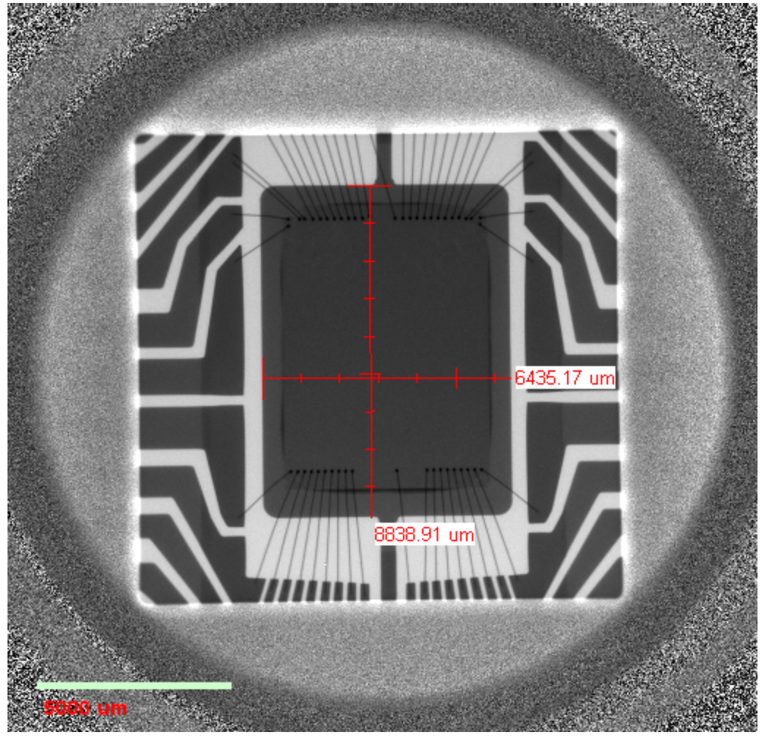
All Samples look the same at optical level except for :

Sample 2 scratch on marking over numbers 6 and 1: No Conclusive Evidence

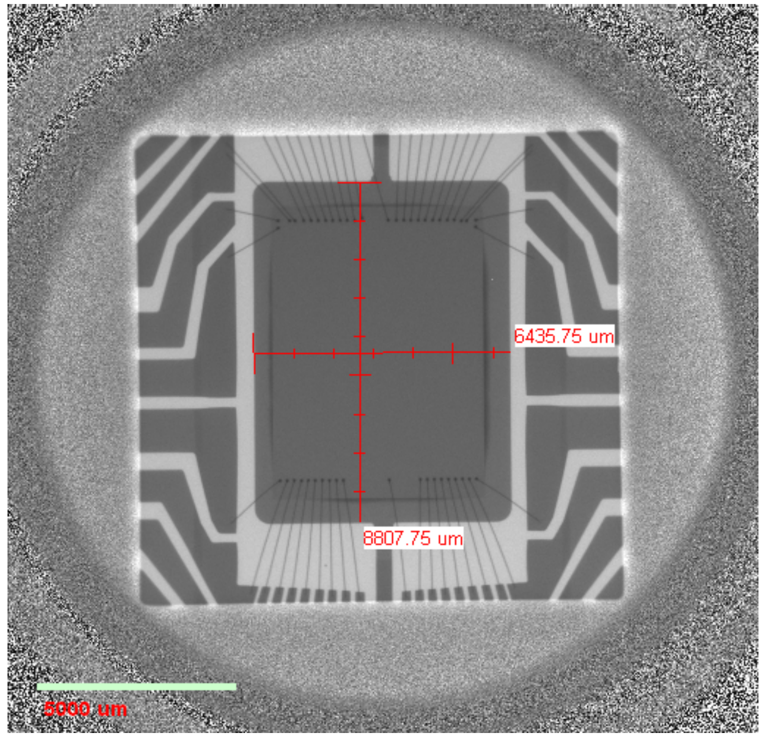


X-ray Analysis / 2D X-ray radiography

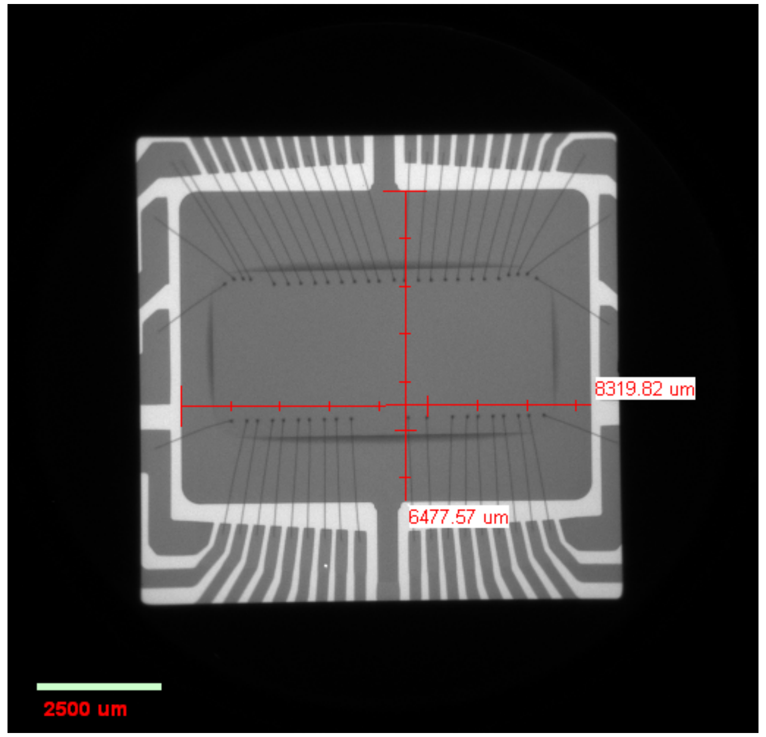
Sample 1



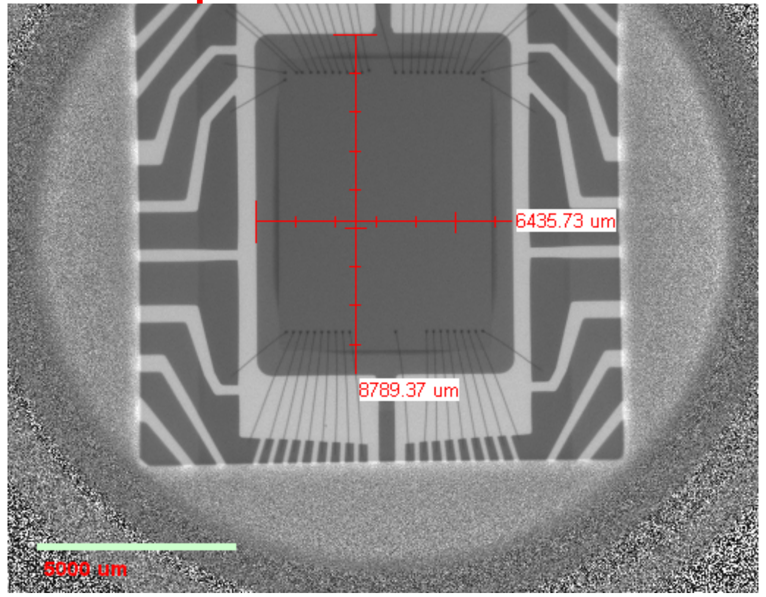
Sample 2



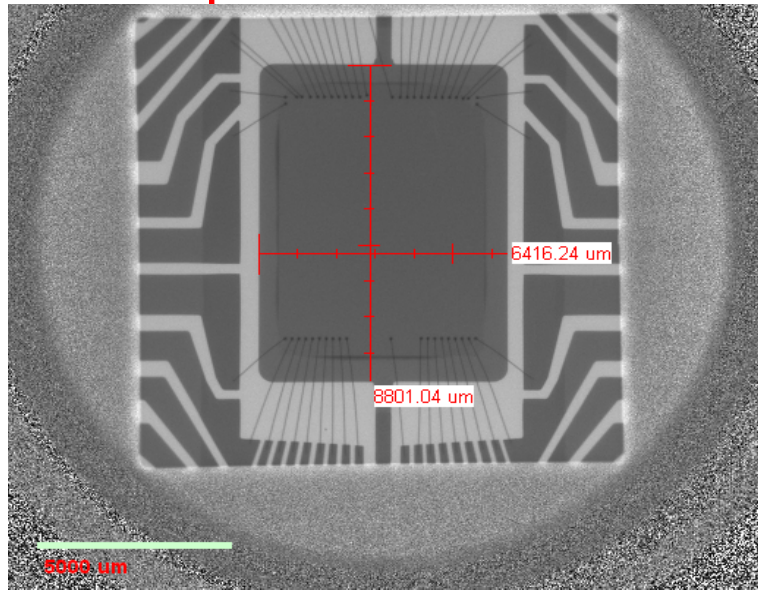
Sample 3



Sample



Sample 5



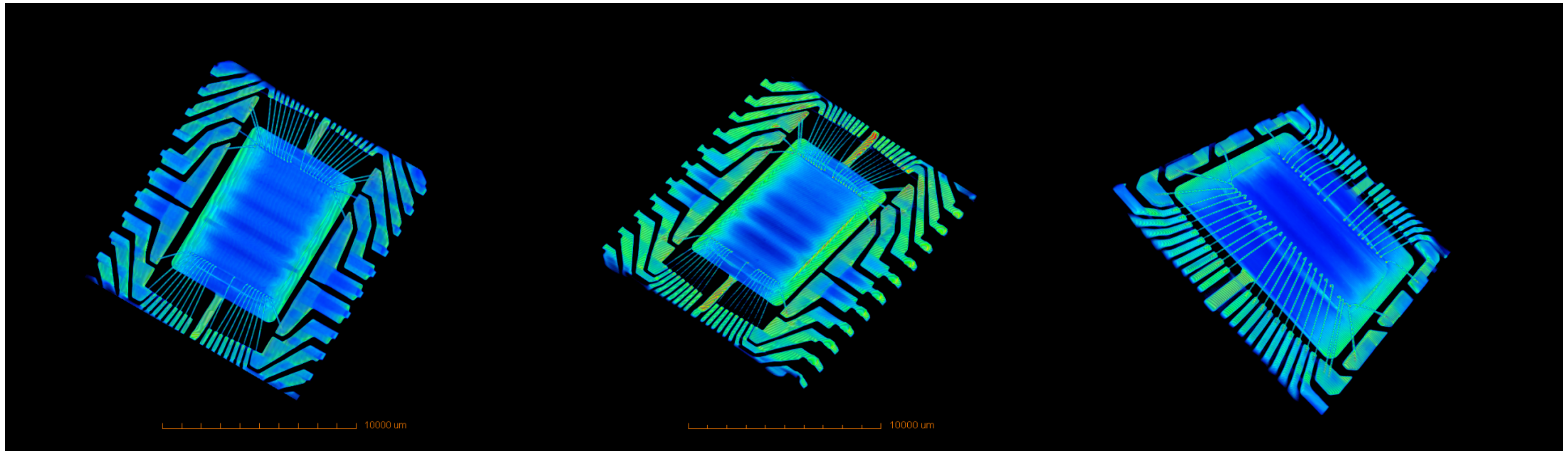
Observation:

Sample 3 has a different Die and bond wires

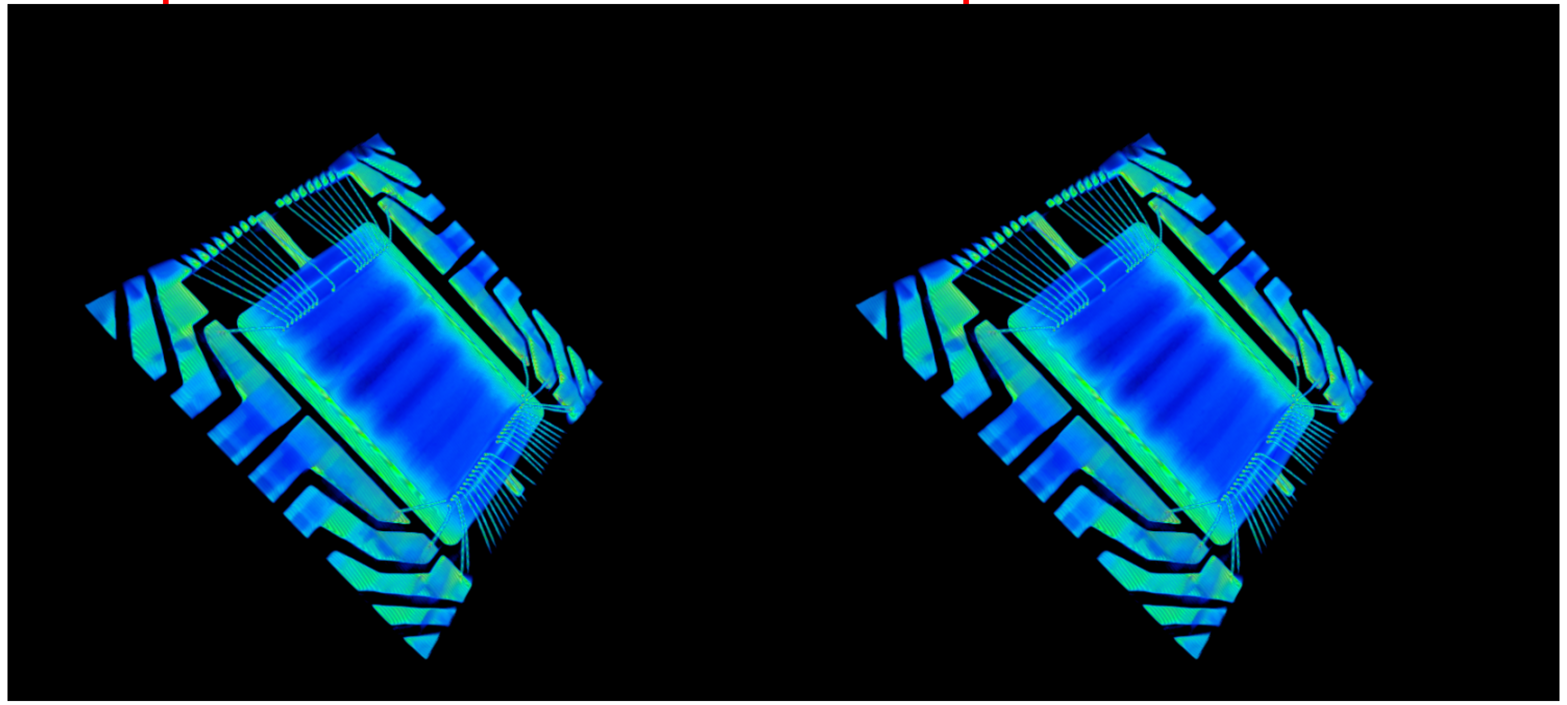
Samples 1,2,4,5 look very similar

X-ray Analysis / 3D X-ray tomography

Sample 1 Sample 2 Sample 3



Sample Sample 5



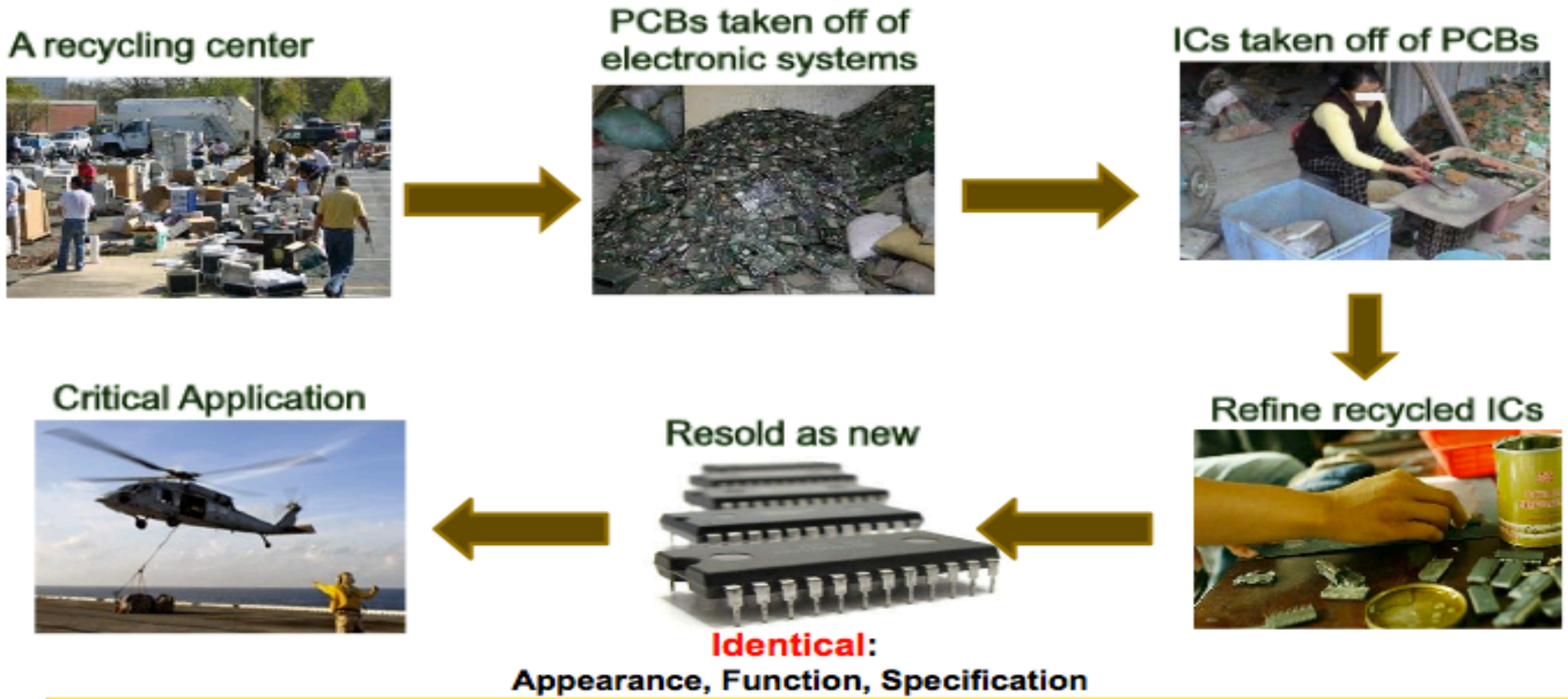
Observation:

All connections are Checked and look fine on all samples

Sample 3 lacks One connection which is believed to be the ground wire. (possible grade issue)

Recycled ICs

- Combating Die/IC Recovery (CDIR) structures
  - Take advantage of circuit aging/degradation in the field
  - Flag if the chip has been mounted on the board and used



A recycling center

PCBs taken off of electronic systems

ICs taken off of PCBs

Refine recycled ICs

Resold as new

Critical Application

Identical: Appearance, Function, Specification

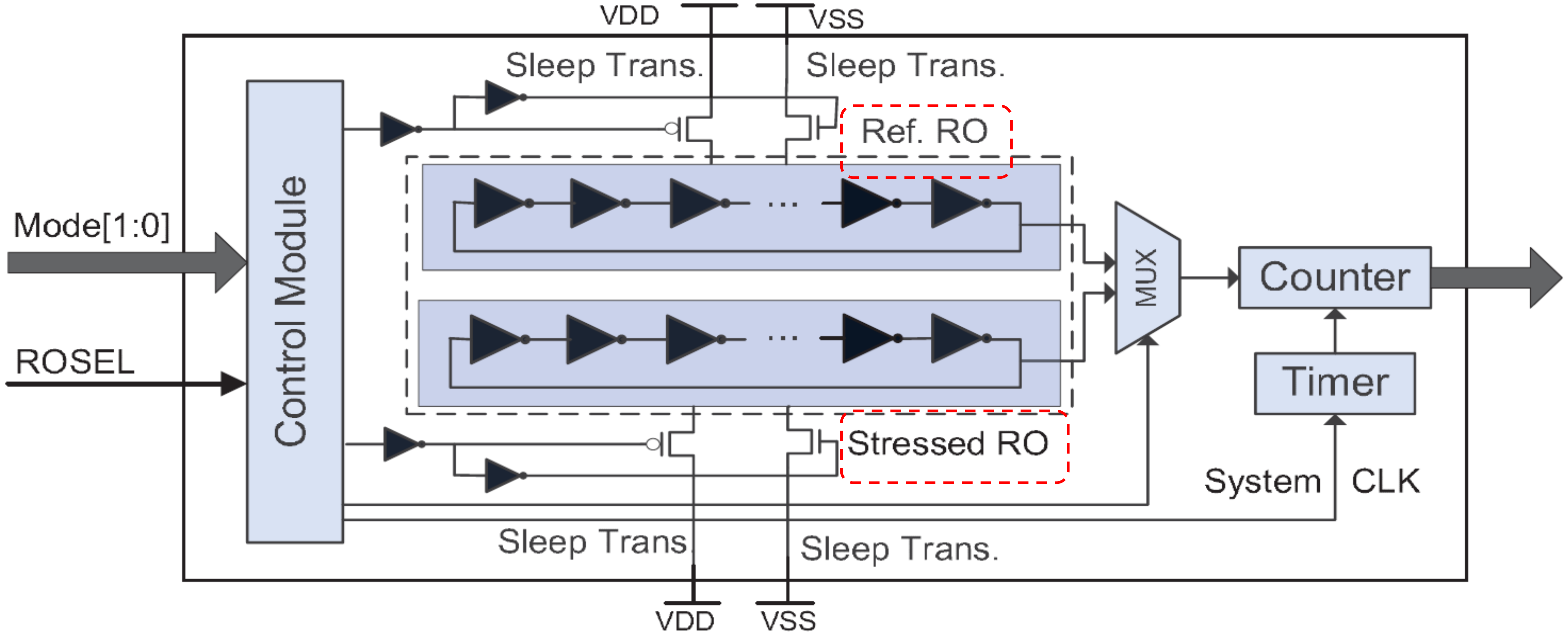
Consumer trends suggest that more gadgets are used in much shorter time – more e-waste

Source: Images are taken from google

RO-CDIR Sensor

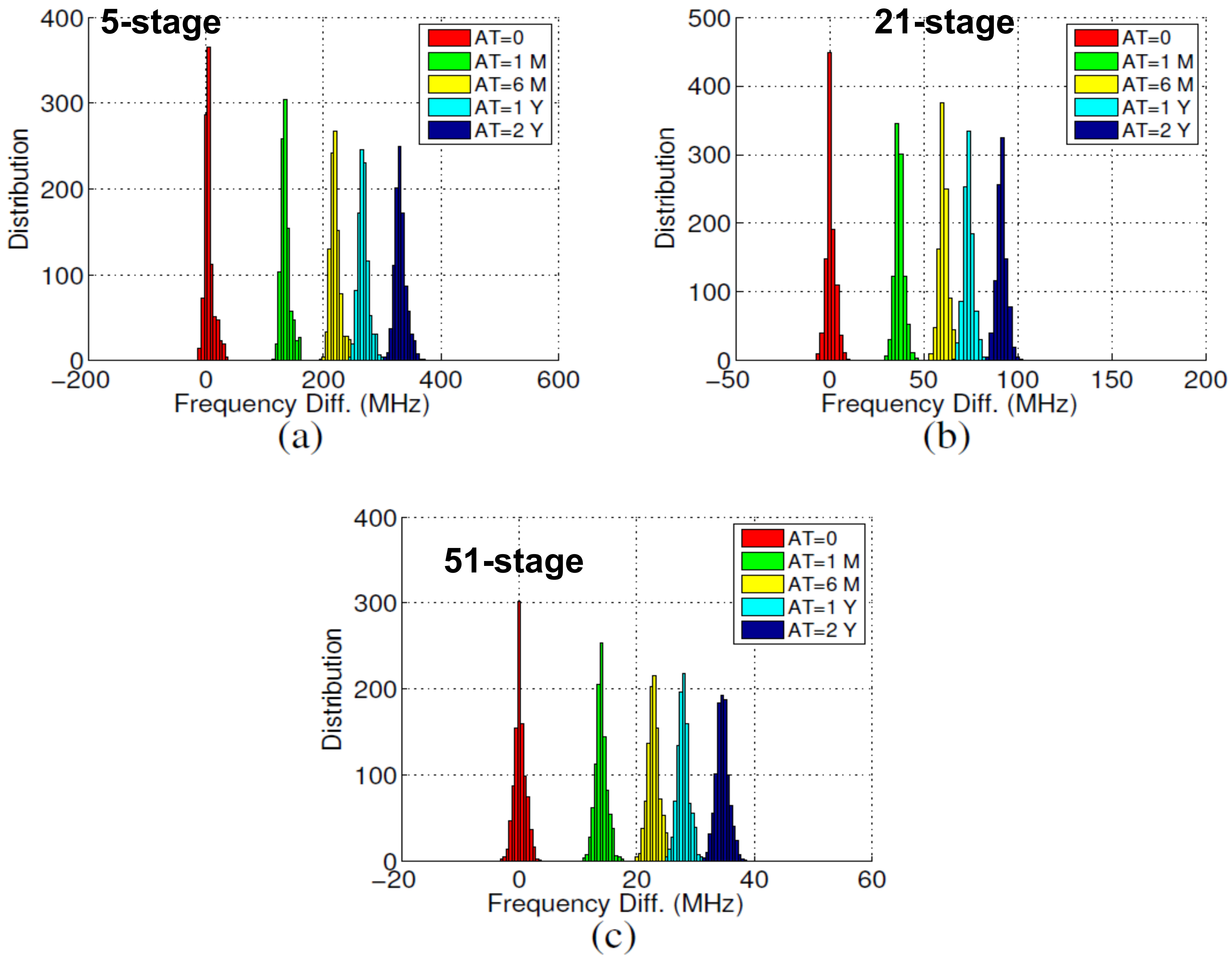
- Combating Die/IC Recovery (CDIR) sensor
  - Ref. RO and Stressed RO
  - Test Mode: Ref. RO and Stressed RO are both off
  - Function Mode: Ref. RO is off while Stressed RO is on
  - Measurement Mode: RO and Stressed RO are both on

X. Zhang and M. Tehranipoor, "**Design of On-chip Light-weight Sensors for Effective Detection of Recycled ICs,**," IEEE Transactions on VLSI (TVLSI), 2013.
X. Zhang, N. Tuzzio, and M. Tehranipoor, "**Identification of Recovered ICs using Fingerprints from a Light-Weight On-Chip Sensor,**" IEEE/ACM Design Automation Conference (DAC), 2012.



Simulation Results

- ROs’ Stage Analysis
  - 90nm Technology (1000 Monte Carlo Simulation)
  - PV: inter-die (2% Tox, 5% Vth, and 5% L) and intra-die (% Tox, 5% Vth, and 5% L)
  - Temperature: 25°c
  - 5-stage, 21-stage,
    and 51-stage ROs



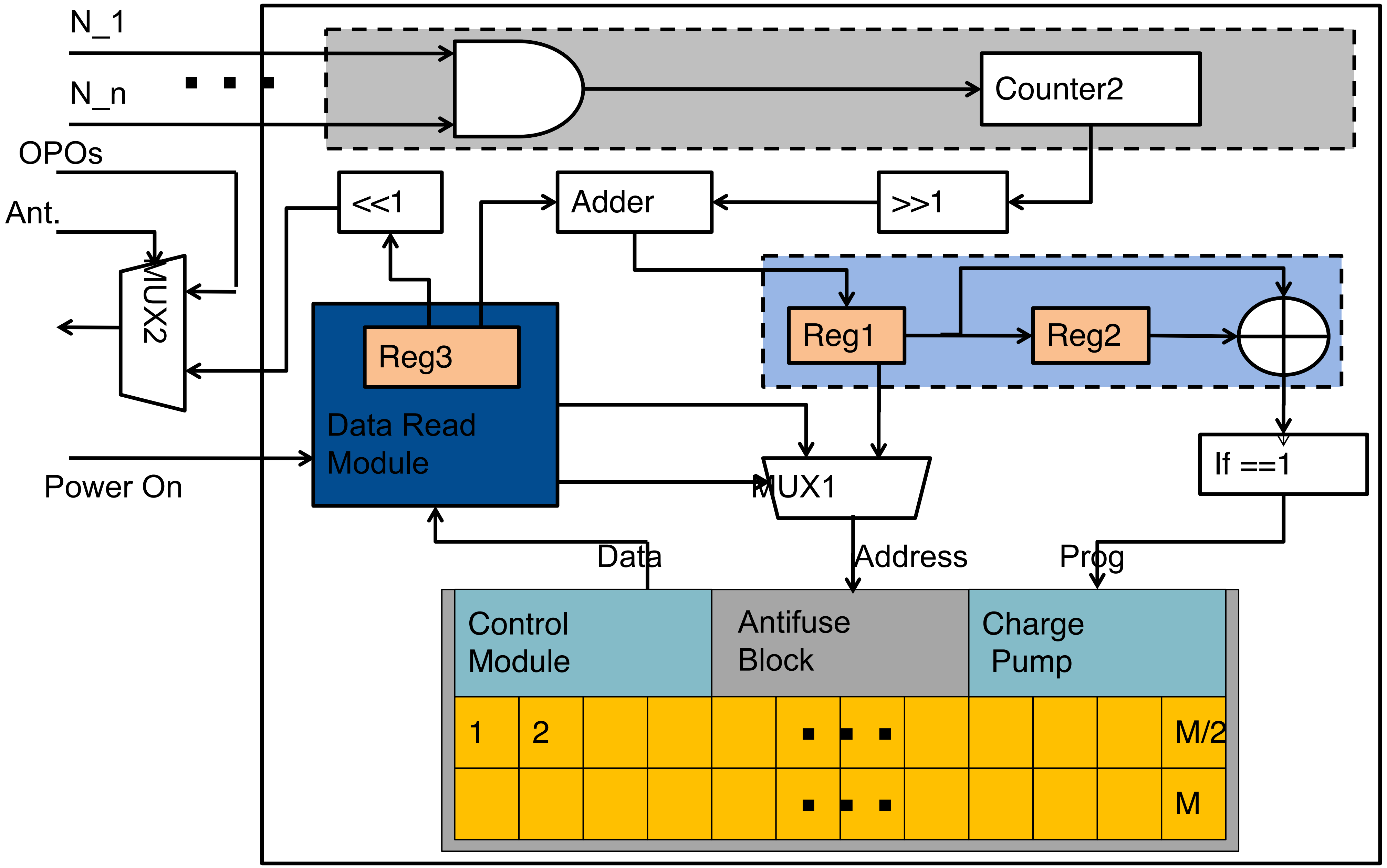
(a)

(b)

(c)

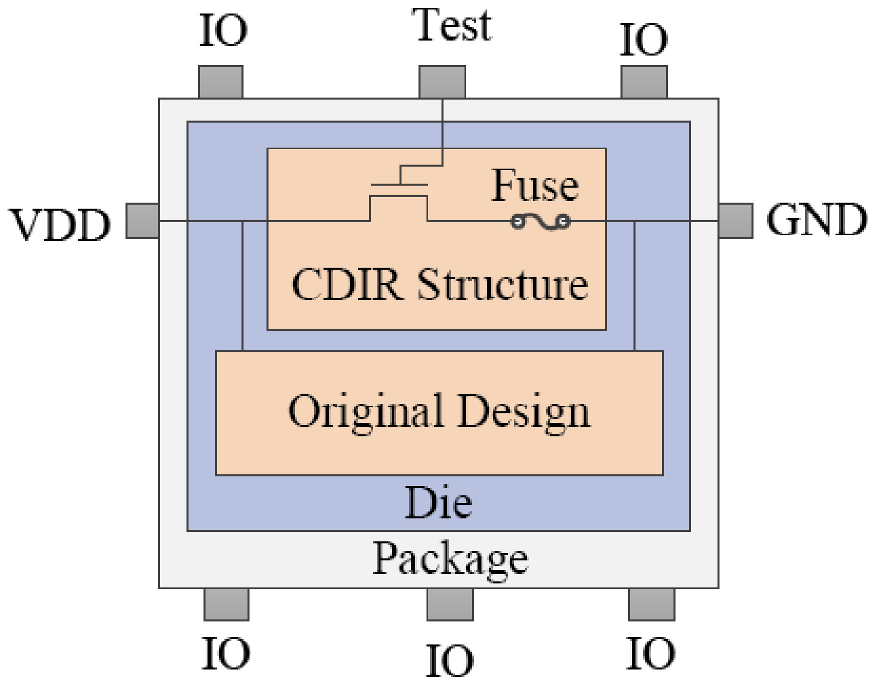
- Detection rate for recovered ICs aged for 1M is 100%
- The stage of ROs does not impact the effectiveness of CDR sensor

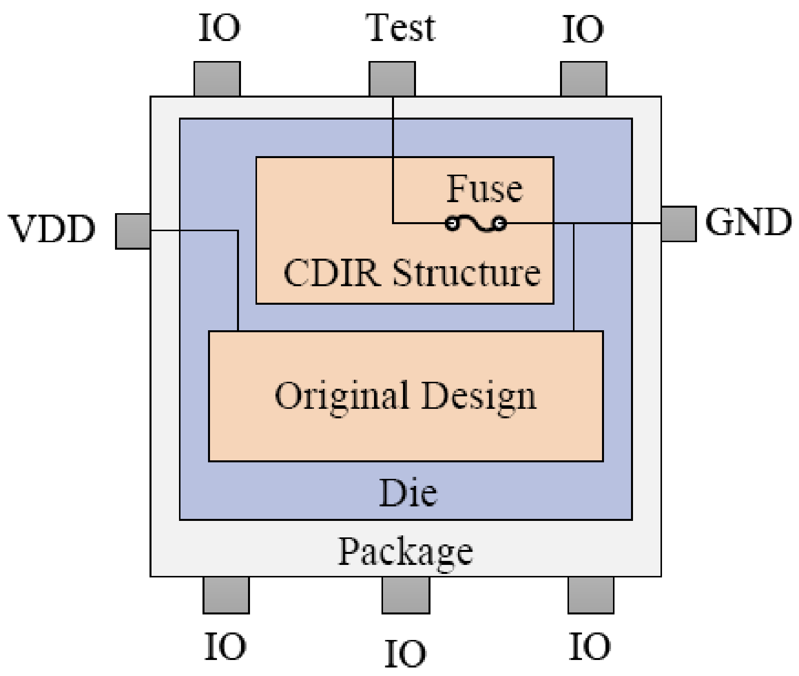
Using Anti-Fuse-based Sensors



X. Zhang, et. al. "**Design of On-chip Light-weight Sensors for Effective Detection of Recycled ICs,**," IEEE Transactions on VLSI (TVLSI), 2013.

Fuse Based – CDIRs



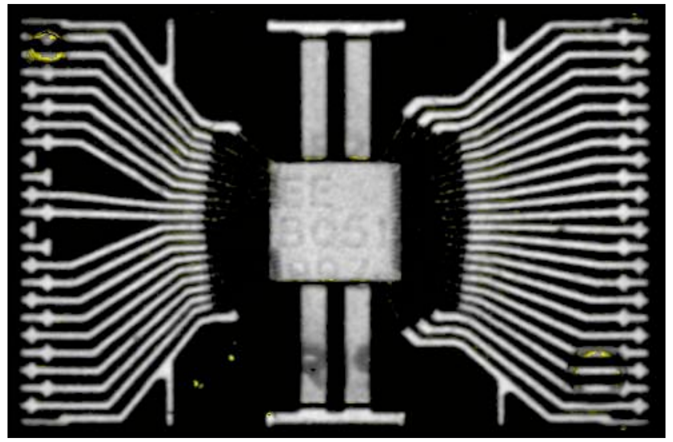


- **The detection of counterfeit (used in the field) components will be performed through the measurement of resistance between**
  - **VDD and GND pins while setting Test pin to VDD for F-CDIR I, and**
  - **Test and GND for F-CDIR II.**
- **If the component has been used before the measured resistance will be high (infinite).**

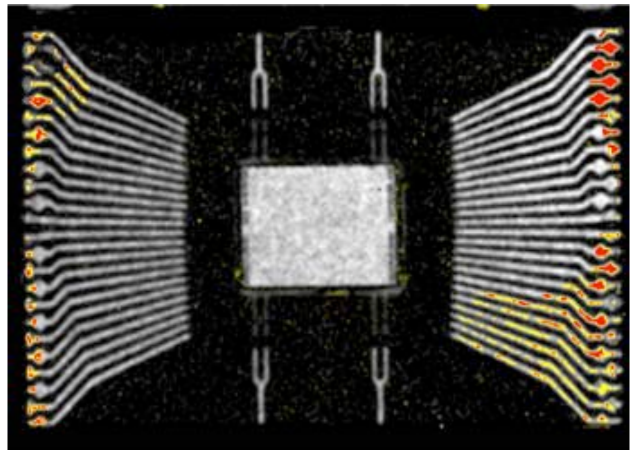
U. Guin, et. al. "**Low-Cost On-Chip Structures for Combating Die and IC Recycling,"** Design Automation Conference (DAC), 2014.

Other Counterfeit Types

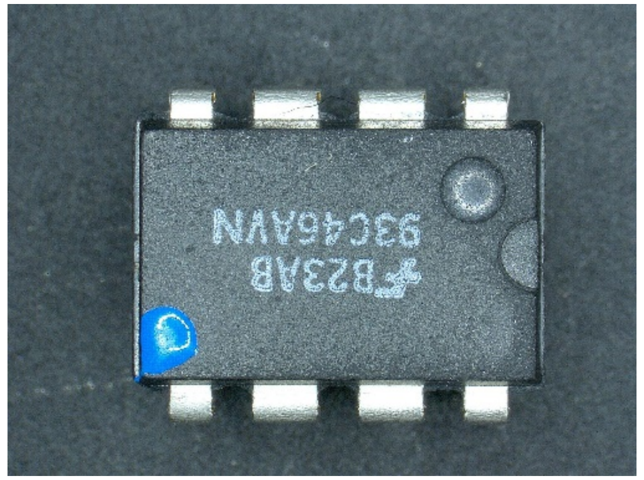
- **Overproduced ICs**: To gain high profit by avoiding IP development
- **Defective ICs**: Defective parts may exhibit correct functionality and difficult to spot in supply chain
- **Out-of-spec ICs**: Rejected and out of spec ICs come to grey market
- **Cloned ICs**: Obtain the design files illegally and clone the device
- **Remarked ICs**: Markings on the package is changed to upgrade the chip (commercial → Military grade)
- **IP Piracy:** Stolen IPs are fabricated and placed in the market as either the original OCM's name or under a different name



Authentic



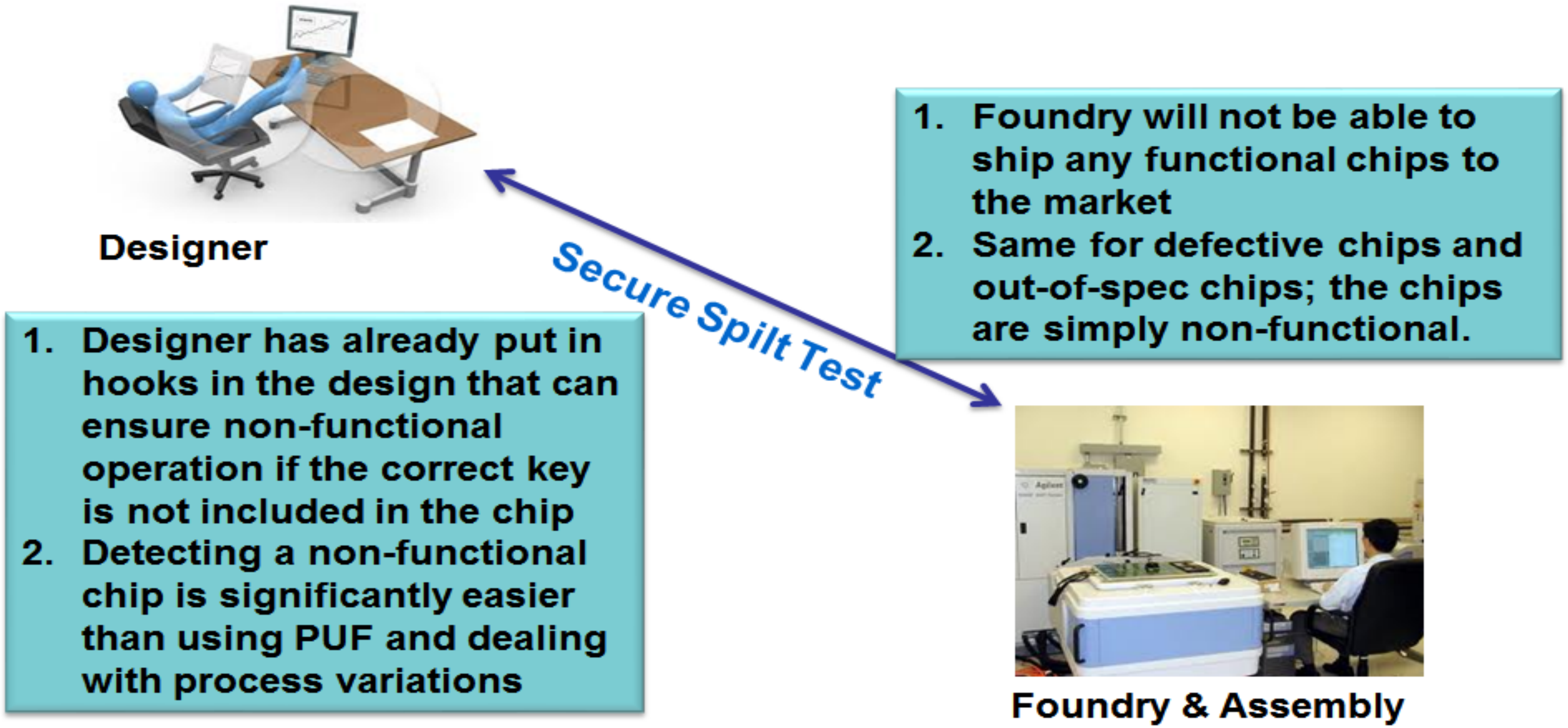
Counterfeit



Remarked

Images: google.com

Secure Split-Test (SST) – HW Metering



1. Designer has already put in hooks in the design that can ensure non-functional operation if the correct key is not included in the chip
2. Detecting a non-functional chip is significantly easier than using PUF and dealing with process variations

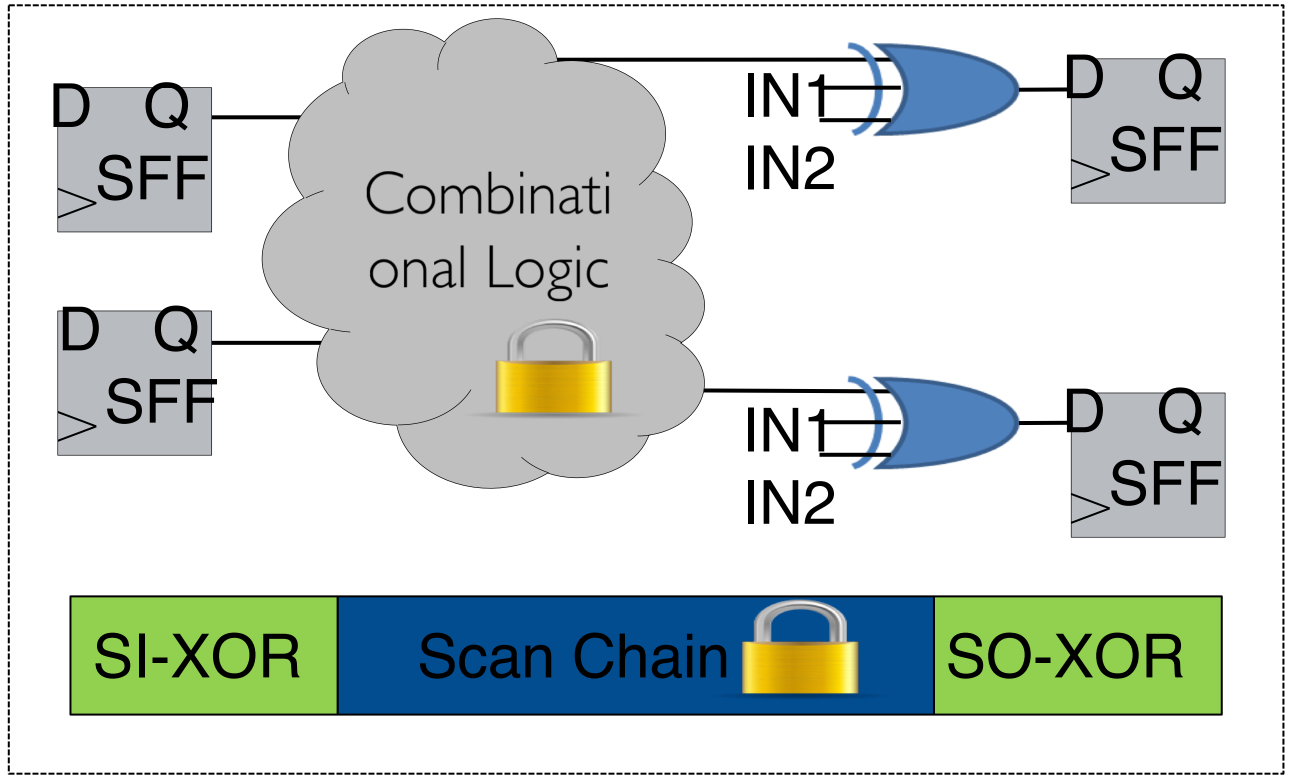
1. Foundry will not be able to ship any functional chips to the market
2. Same for defective chips and out-of-spec chips; the chips are simply non-functional.

G. Contreras et. al., "**Secure Split-Test for preventing IC piracy by untrusted foundry and assembly**," *IEEE International Symposium Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT),* pp.196-203, 2013.

T. Rahman, et. al., "**CSST: Preventing Distribution of Unlicensed and Rejected ICs by Untrusted Foundry and Assembly,**" IEEE Int. Symposium on Defect and Fault Tolerance Symposium (DFTS), Oct. 2014

SST Requirements

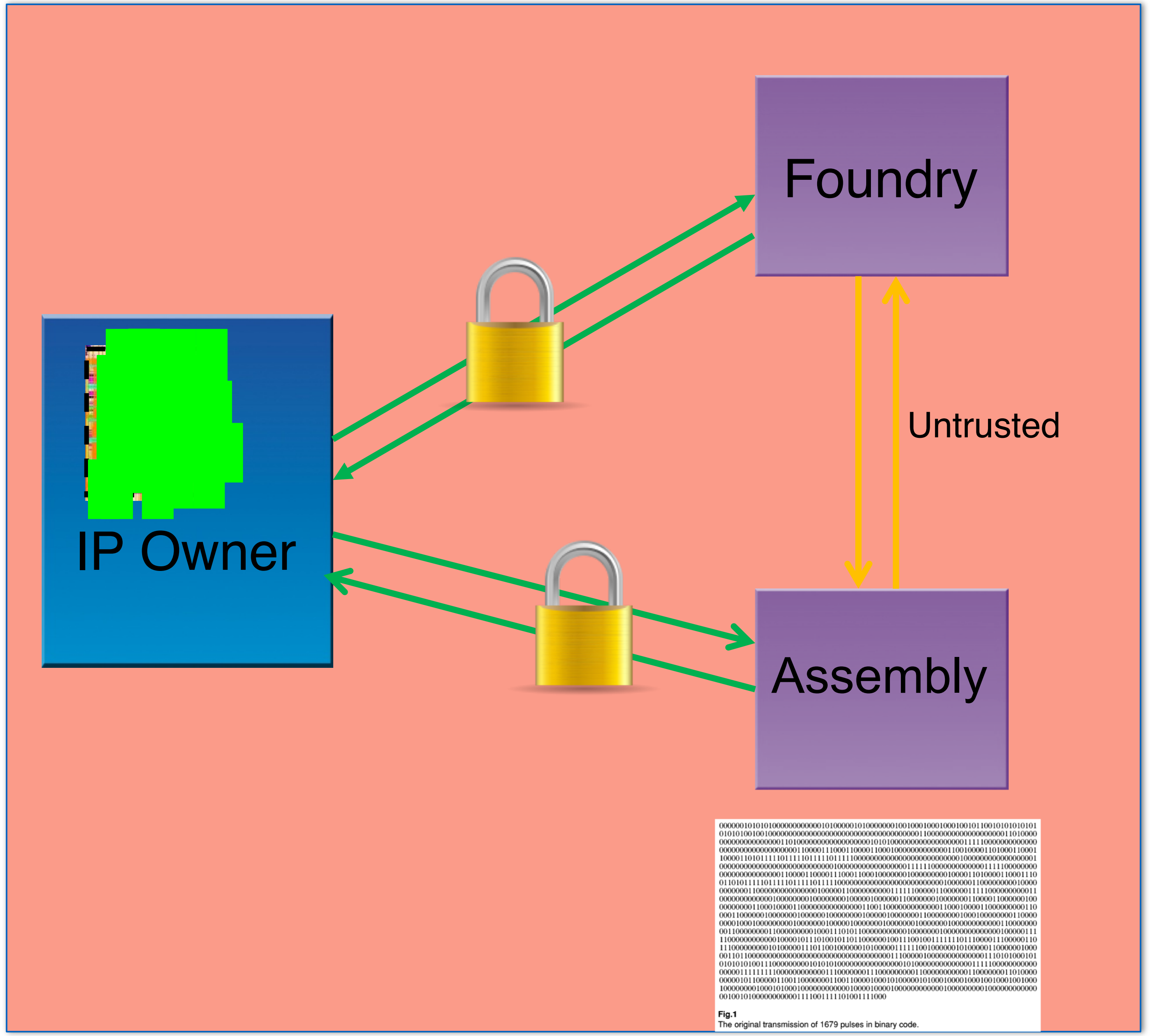
- Signature or response for each IC has to be different (and random)
- Provides functional-locking capability
- Provides scan locking mechanism
- Easy to implement, difficult to break
- Provides easy detection
- Easy communication between foundry/assembly and IP owner
- Ensure resiliency against different type of attacks



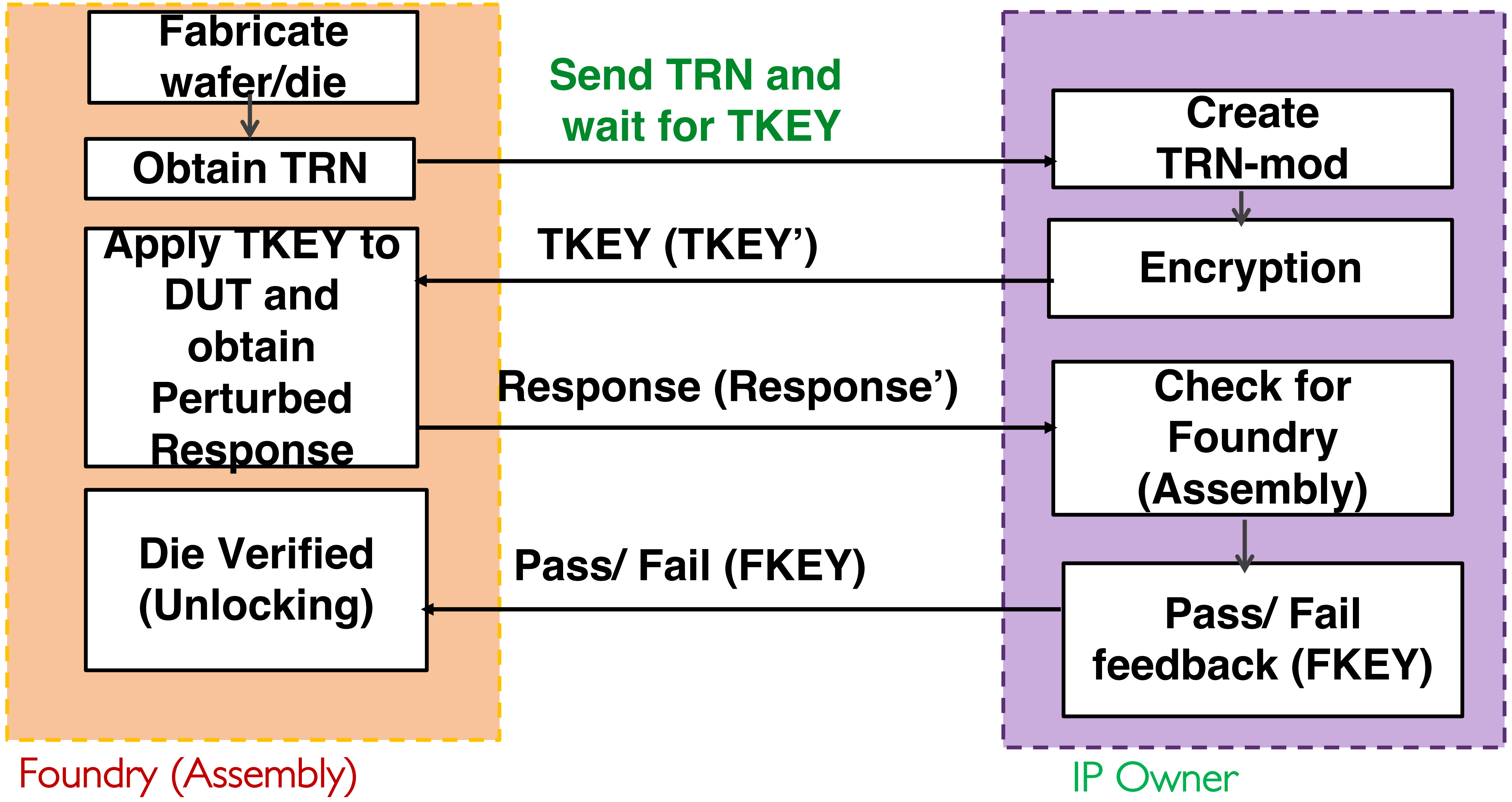
Logic Obfuscation
Scan Chain Obfuscation

SST Overview

- Detecting and preventing over produced, defective or out-of-spec ICs by untrusted foundry and assembly.
- Trust between IP owner and foundry/assembly w/o physical presence.
- IP owner controls production.
- Ensure unauthorized ICs are non-functional and can easily be detected if they are in market.

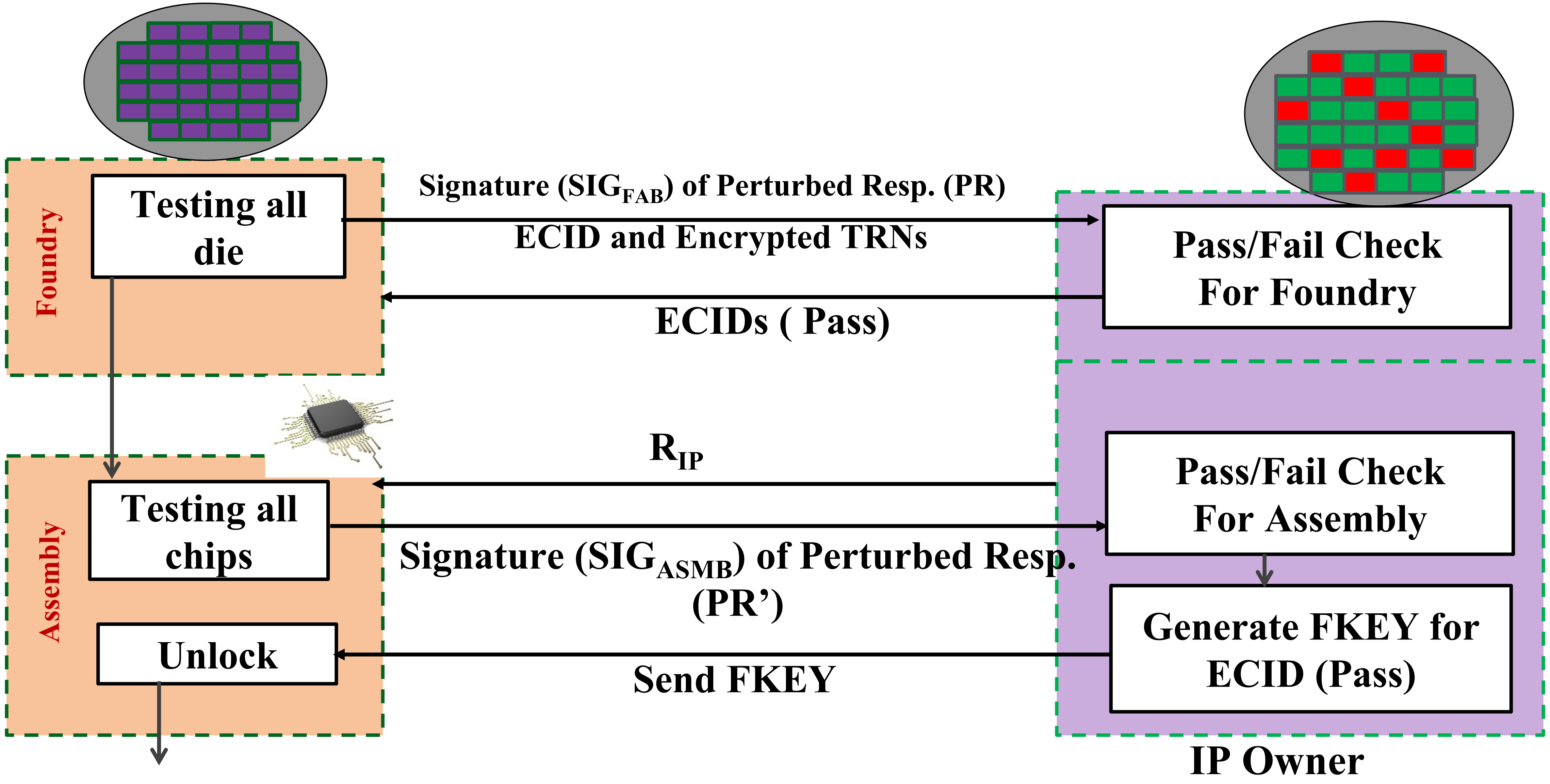


Original SST



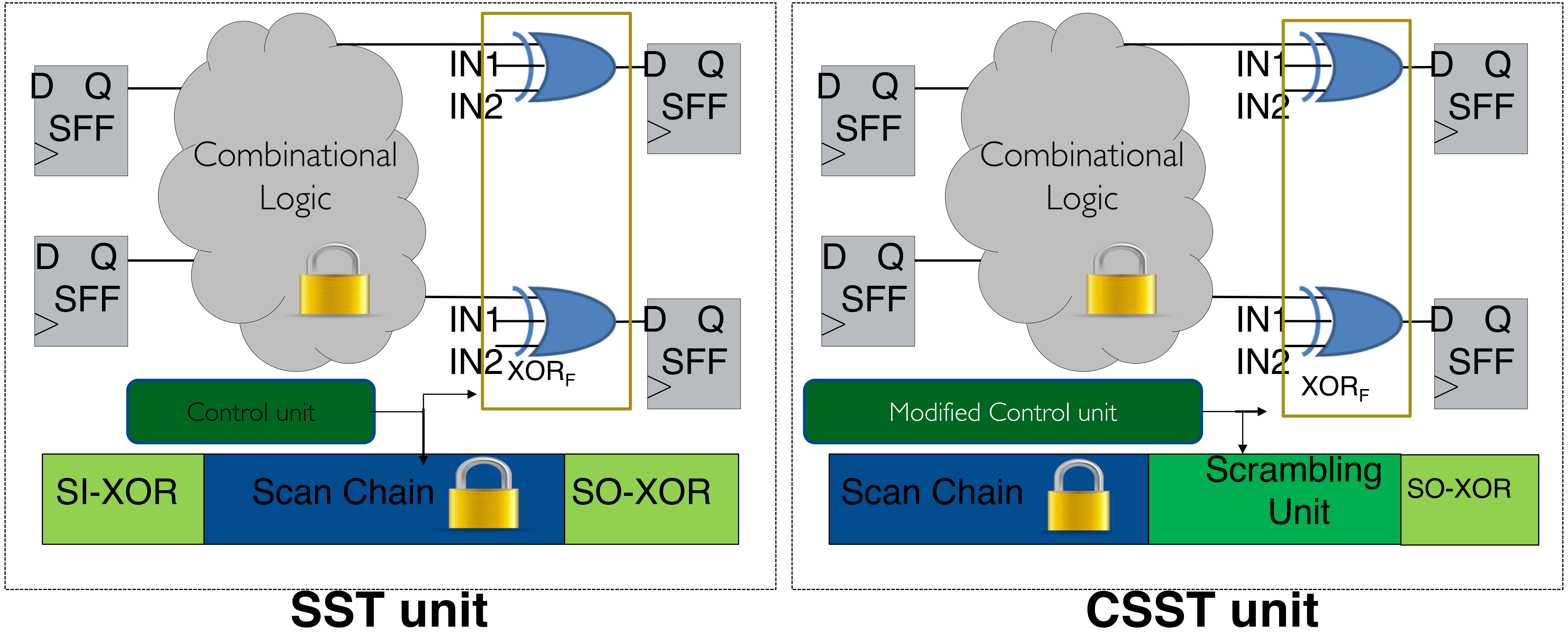
- Communication is required for each die and each chip.
- Significant test time overhead.
- Large amount of data to be transferred between parties.
- RSA decryption during testing.

CSST


Foundry
Testing all die
Signature (SIG_{FAB}) of Perturbed Resp. (PR)
ECID and Encrypted TRNs
Pass/Fail Check For Foundry
ECIDs (Pass)
R_{IP}
Assembly
Testing all chips
Pass/Fail Check For Assembly
Signature (SIG_{ASMB}) of Perturbed Resp. (PR')
Generate FKEY for ECID (Pass)
Unlock
Send FKEY
IP Owner

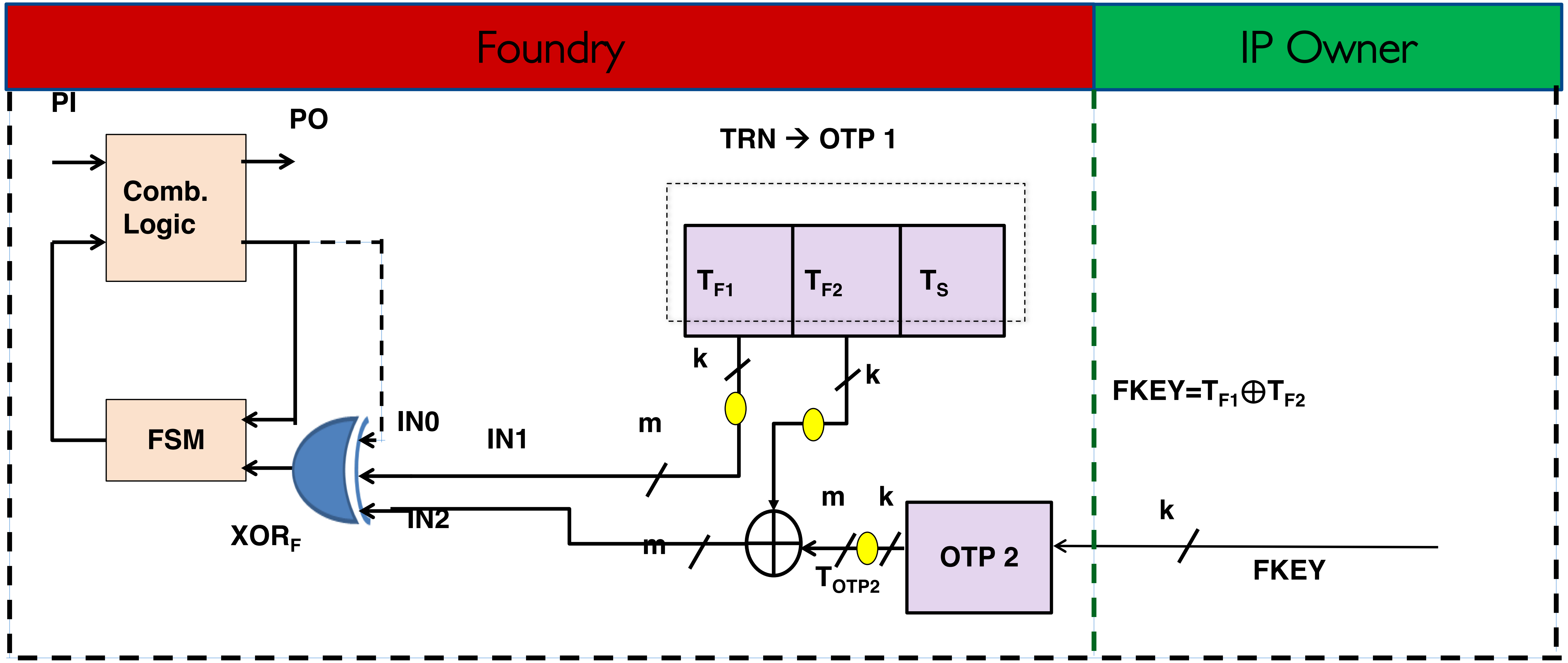
CSST removes the complex communication between foundry/assembly and IP owner significantly.

SST vs. CSST Locking



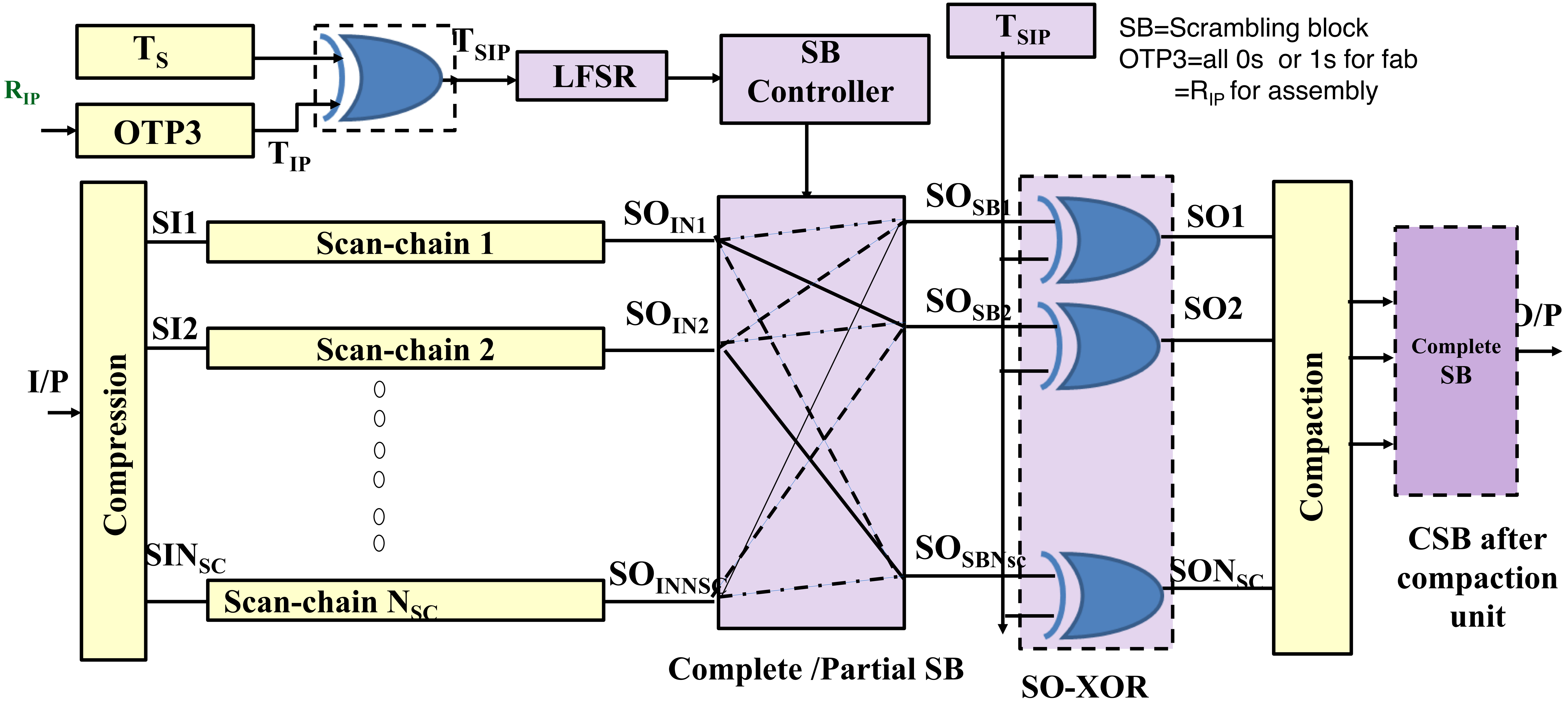
- TRN controls XOR$_F$ block.
- Modified control unit controls scrambling and SO-XOR blocks.

CSST: Functional Locking



- XORs are inserted on non-critical paths
- Foundry does not need any TKEY for testing.
- FKEY does not reveal TRN value.

CSST: Scan Locking



SB=Scrambling block

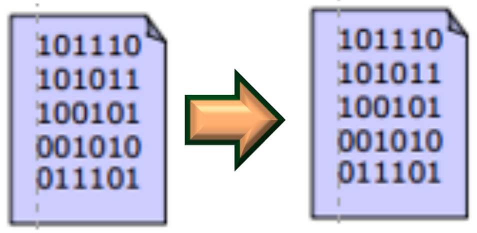
OTP3=all 0s or 1s for fab

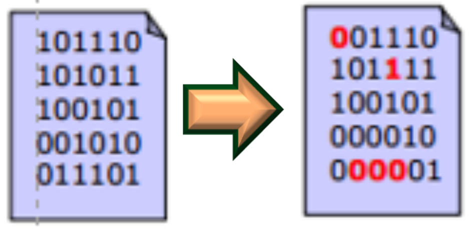
=R_{IP} for assembly

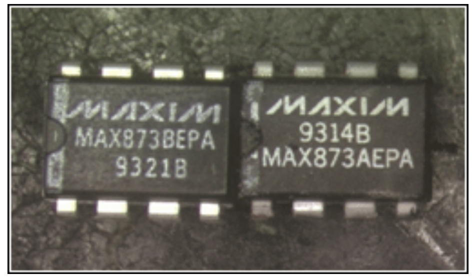
- Scrambling block adds another layer of security.
- More robust to attacks.
- CSB/PSB could be added after compaction

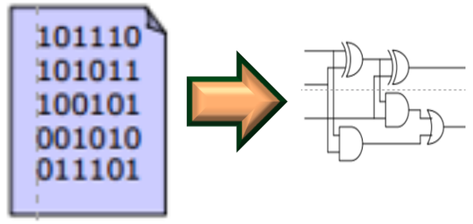
SST Summary

Cloning	Can’t clone because they don’t know the exact key / TRNG
HW Trojan	Difficult: Functionality is unknown
Overbuilding	Owners have full of control
Remarking	ECID contain chip grade info
Reverse Engineering	TRNG is unclonable

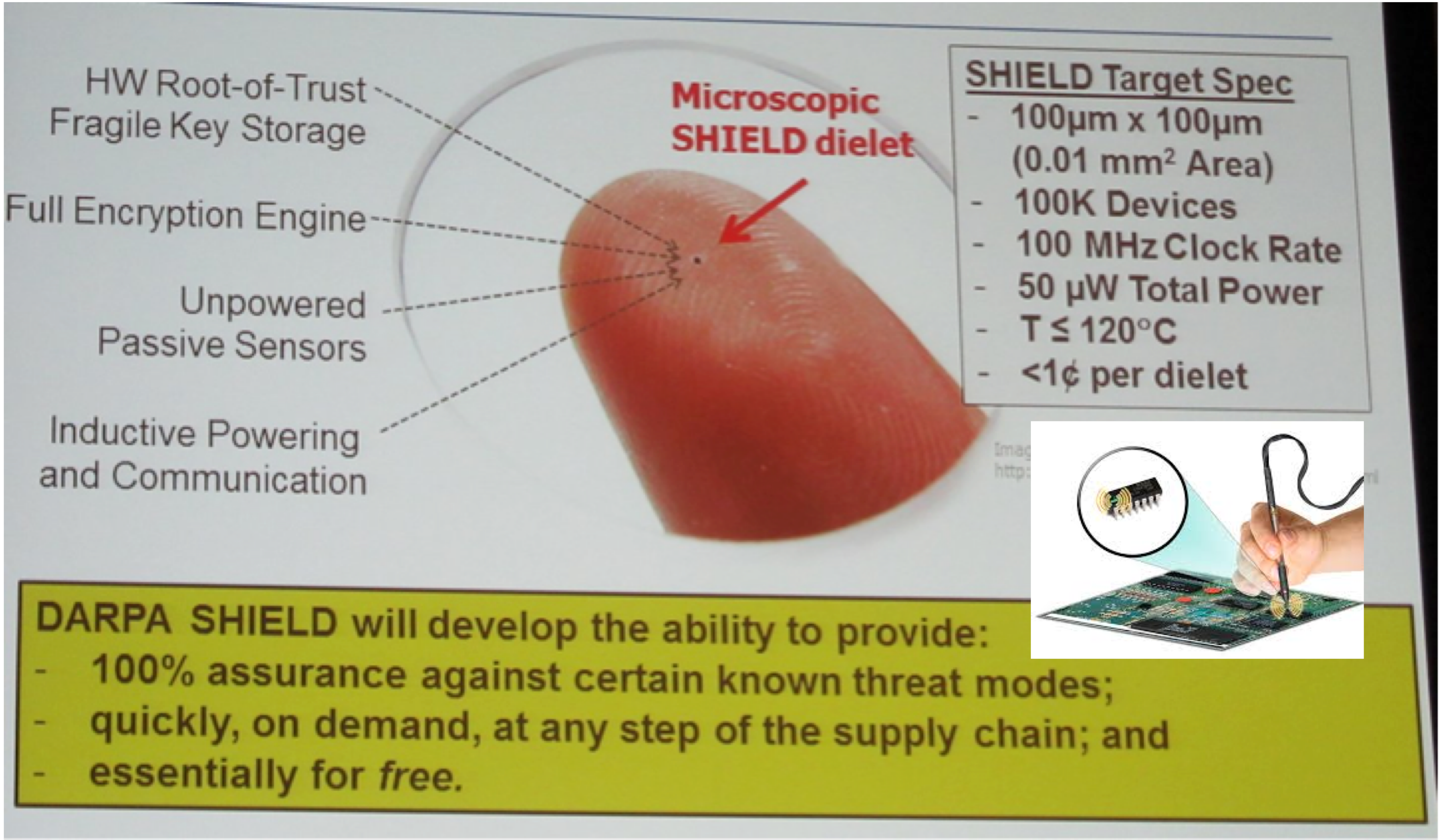








DARPA SHIELD



HW Root-of-Trust
Fragile Key Storage

Full Encryption Engine

Unpowered
Passive Sensors

Inductive Powering
and Communication

Microscopic SHIELD dielet

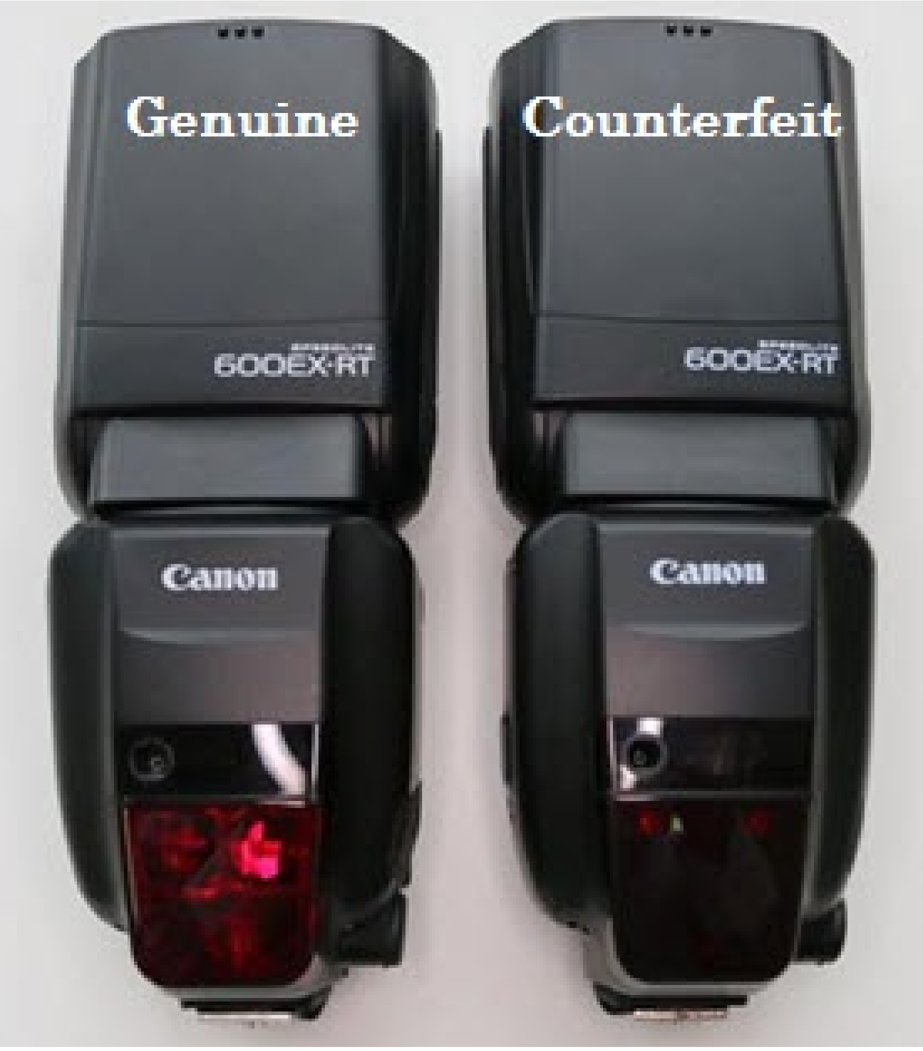
SHIELD Target Spec

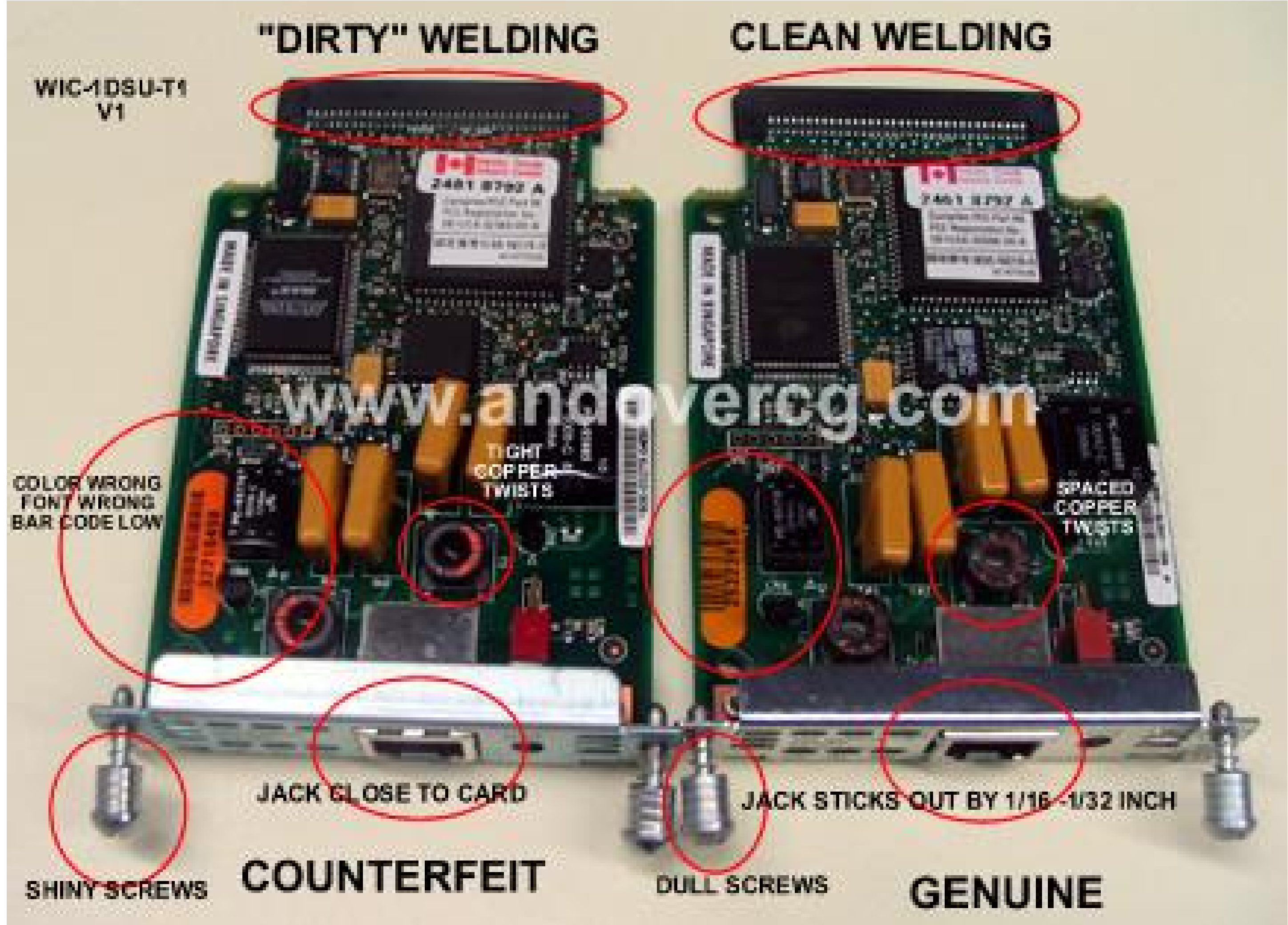
- 100µm x 100µm (0.01 mm^2 Area)
- 100K Devices
- 100 MHz Clock Rate
- 50 µW Total Power
- T ≤ 120°C
- <1¢ per dielet

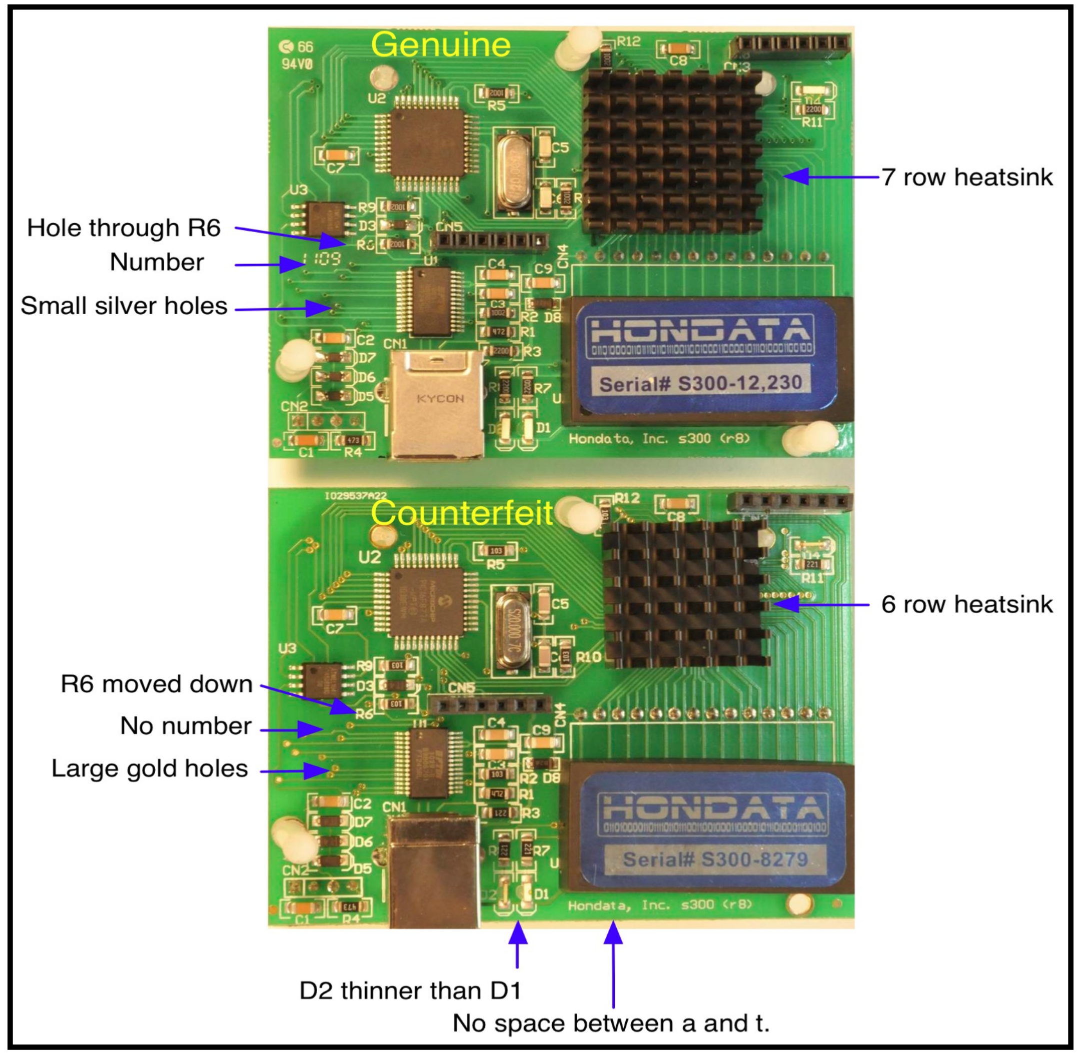
DARPA SHIELD will develop the ability to provide:

- 100% assurance against certain known threat modes;
- quickly, on demand, at any step of the supply chain; and
- essentially for *free.*

The Rise of Clones







Genuine vs. Fake Canon Speedlite 600EX-RT flash

Genuine vs. Fake Cisco router

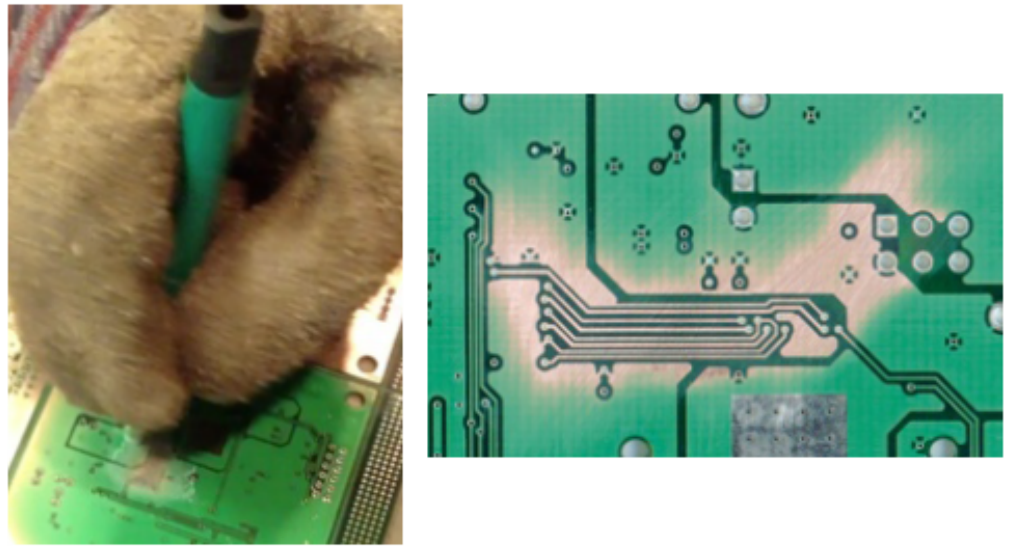
Genuine vs. Fake Honda S300 PCB, as plug-in to the engine control unit

Destructive Reverse Engineering

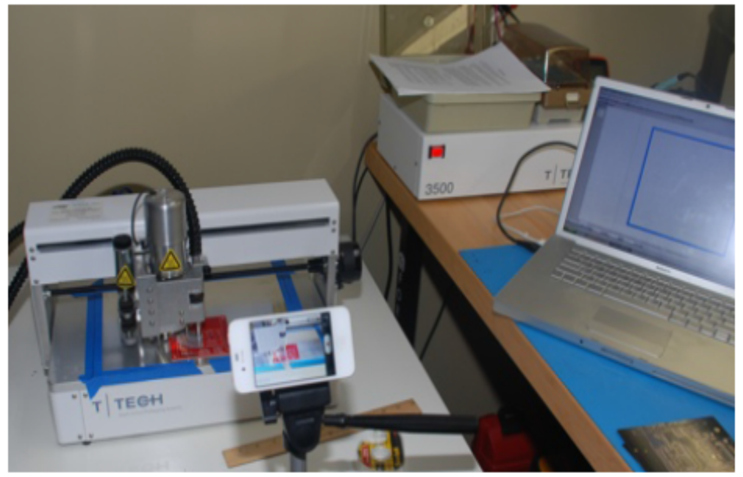
Using Sandpaper

Laser

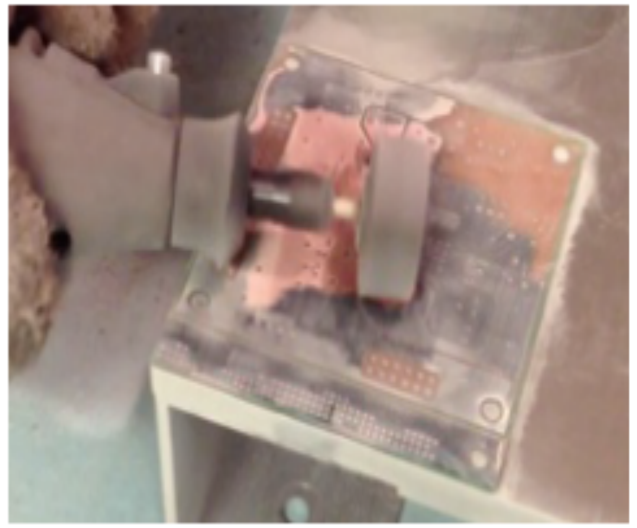
Chemical



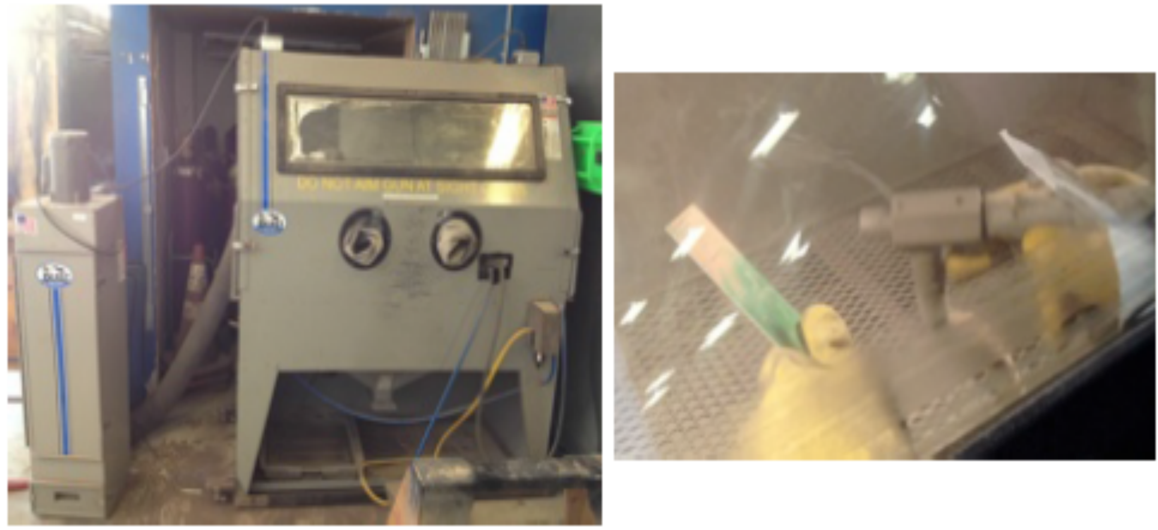
Using Fiberglass Scratch Brush



CNC (computer numerical control)



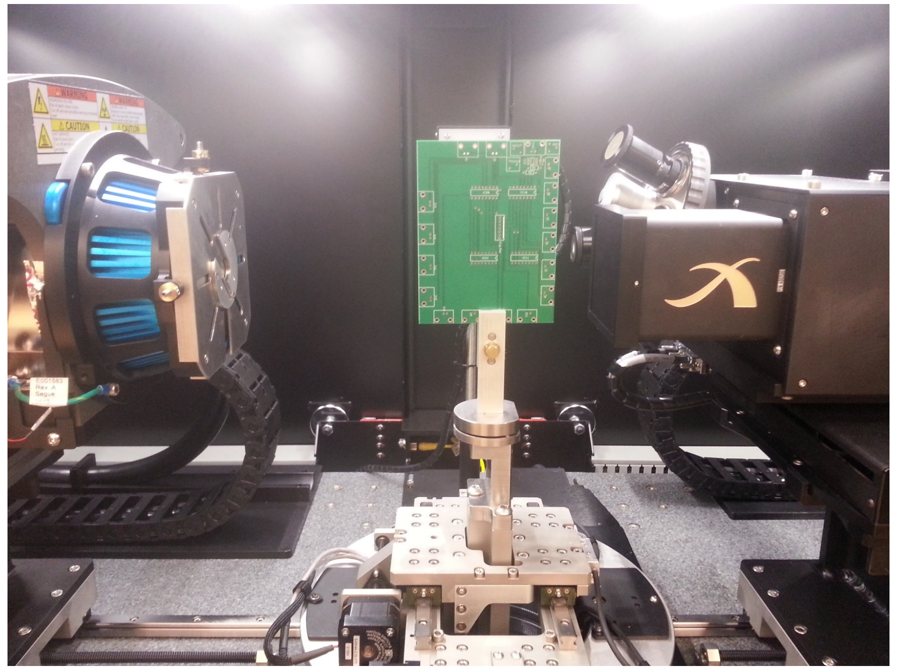
Dremel Tool

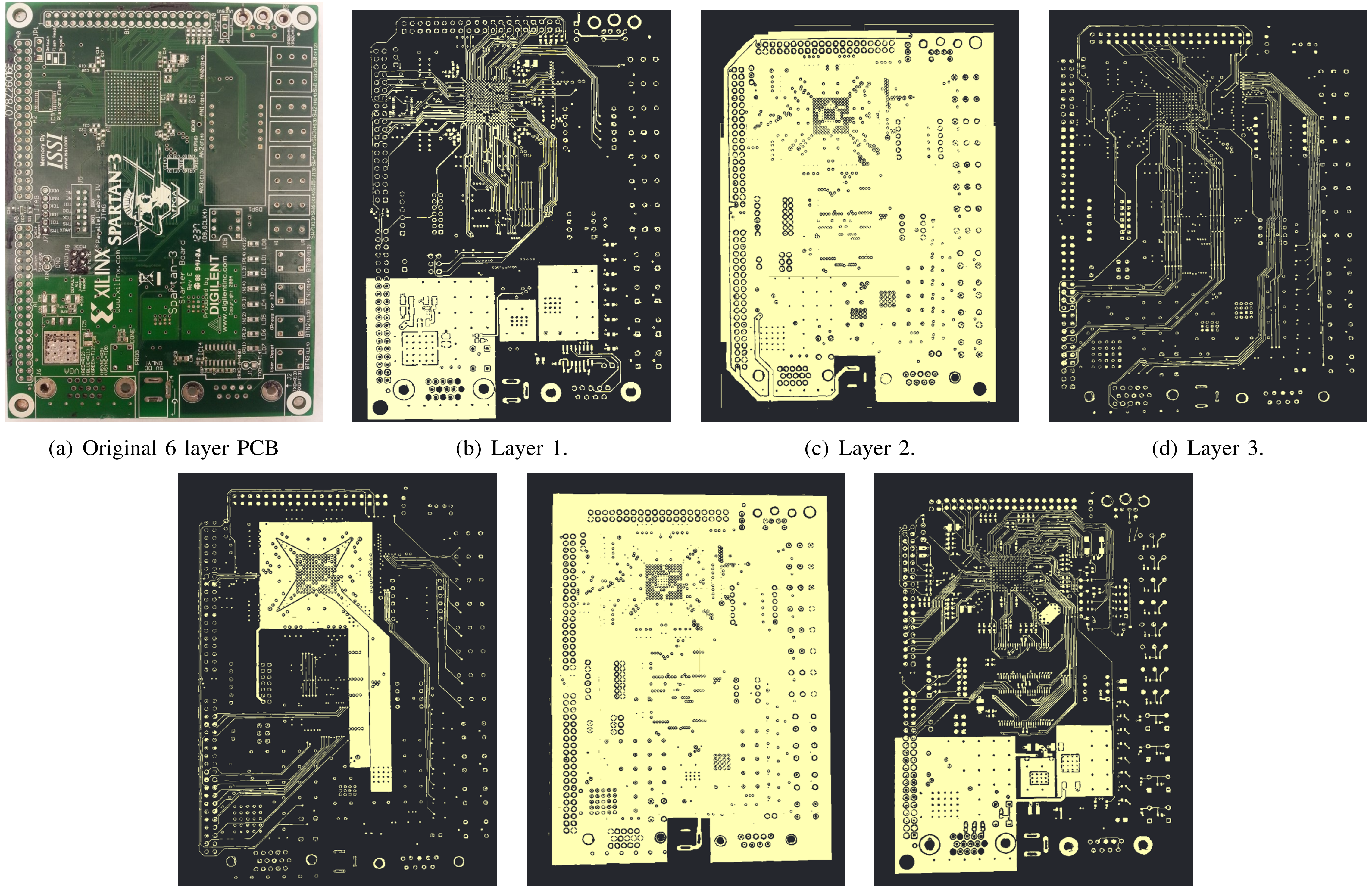


Abrasive Blasting

Joe Grand, USENIX Association, 2014.

Non-destructive Reverse Engineering





(a) Original 6 layer PCB

(b) Layer 1.

(c) Layer 2.

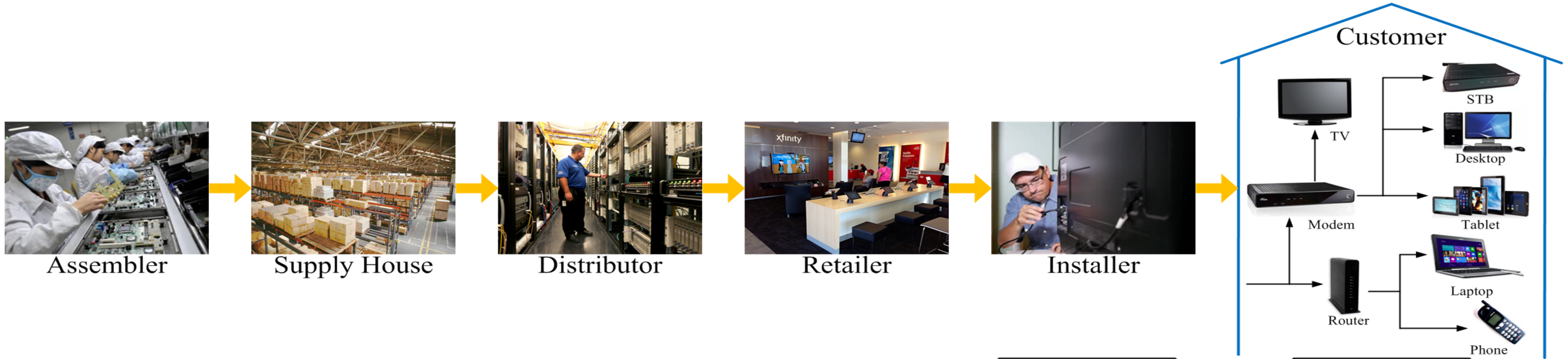
(d) Layer 3.

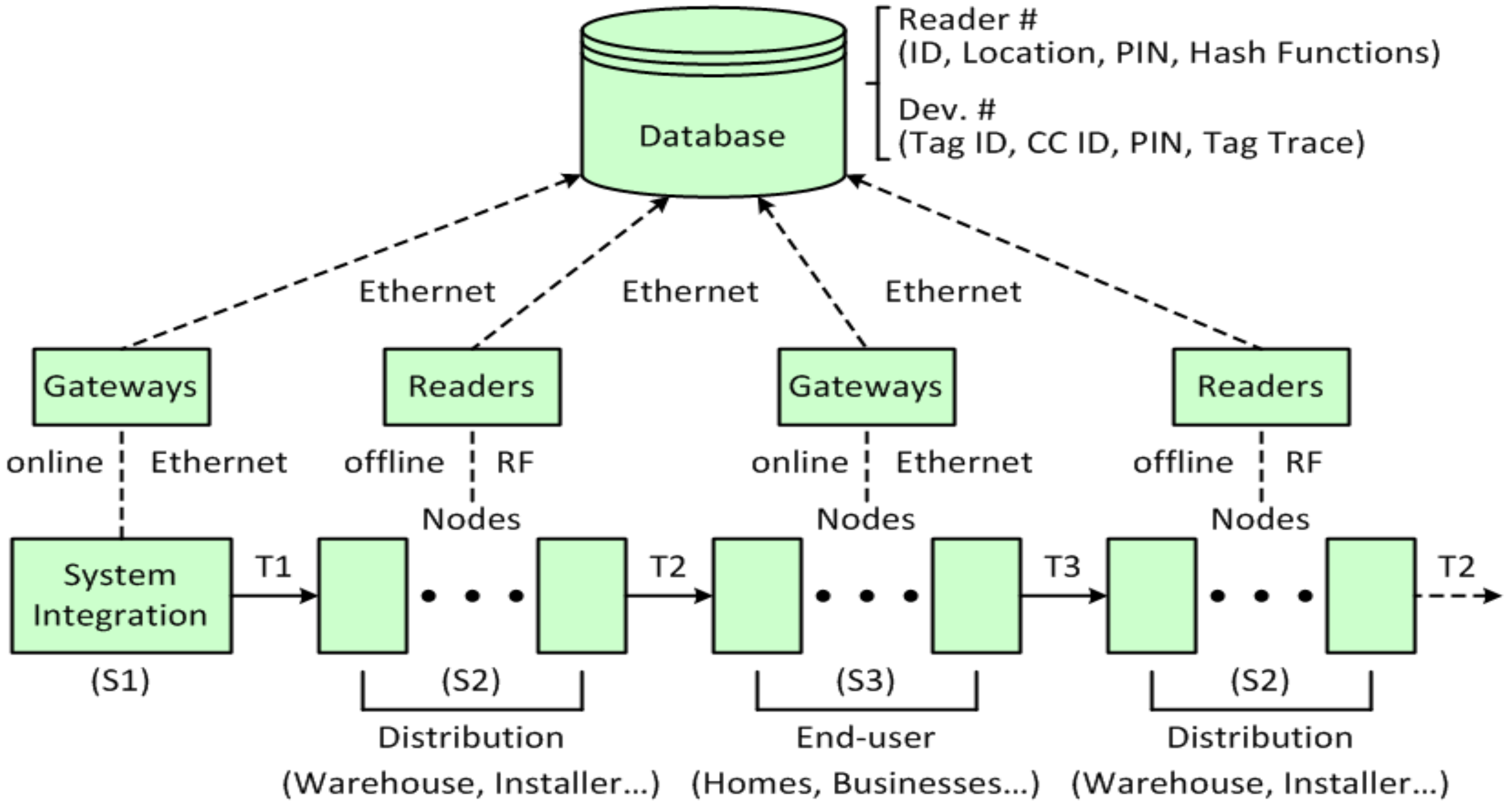
(e) Layer 4.

(f) Layer 5.

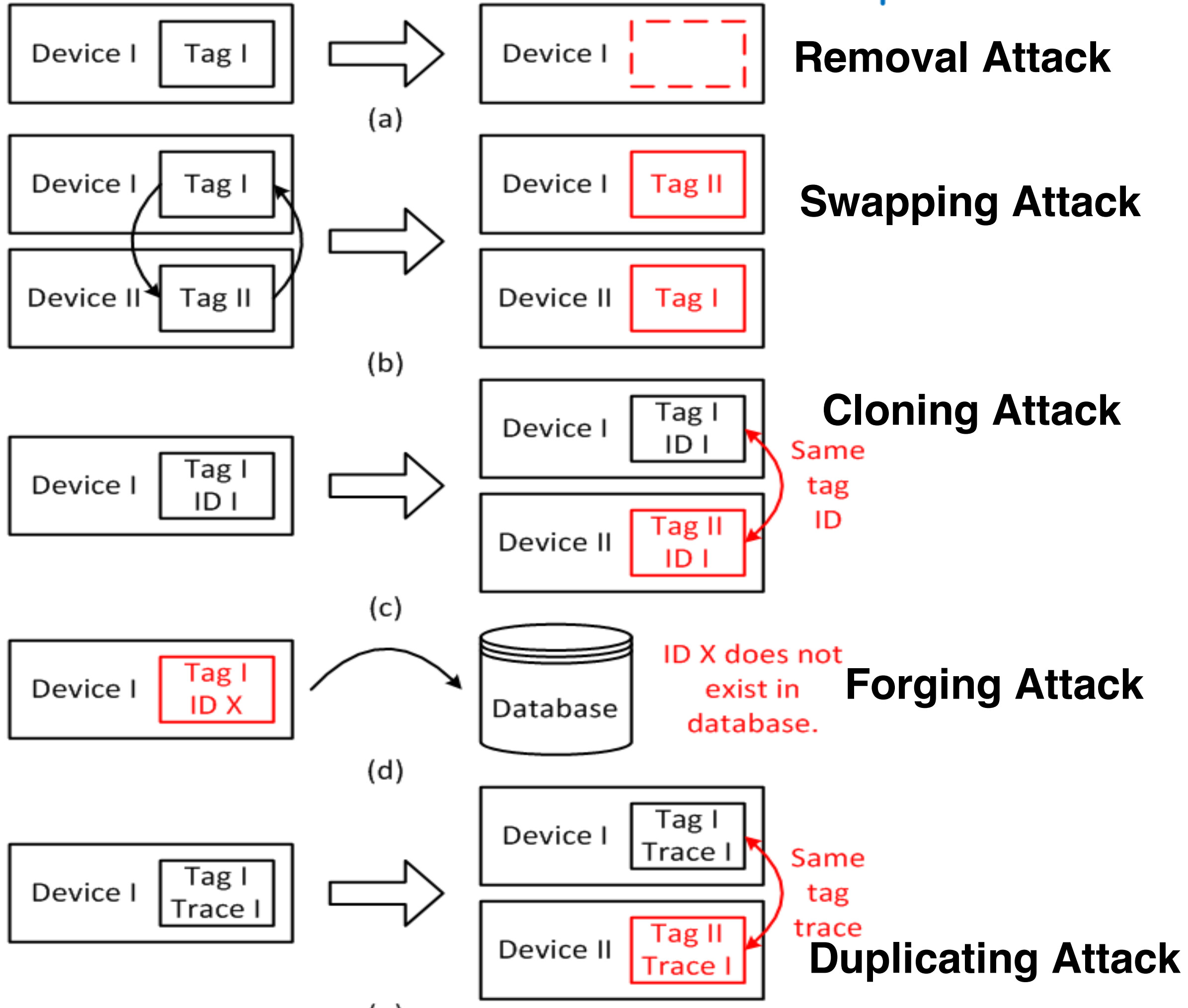
(g) Layer 6.

RFID-Enabled Traceability – On-System Solutions



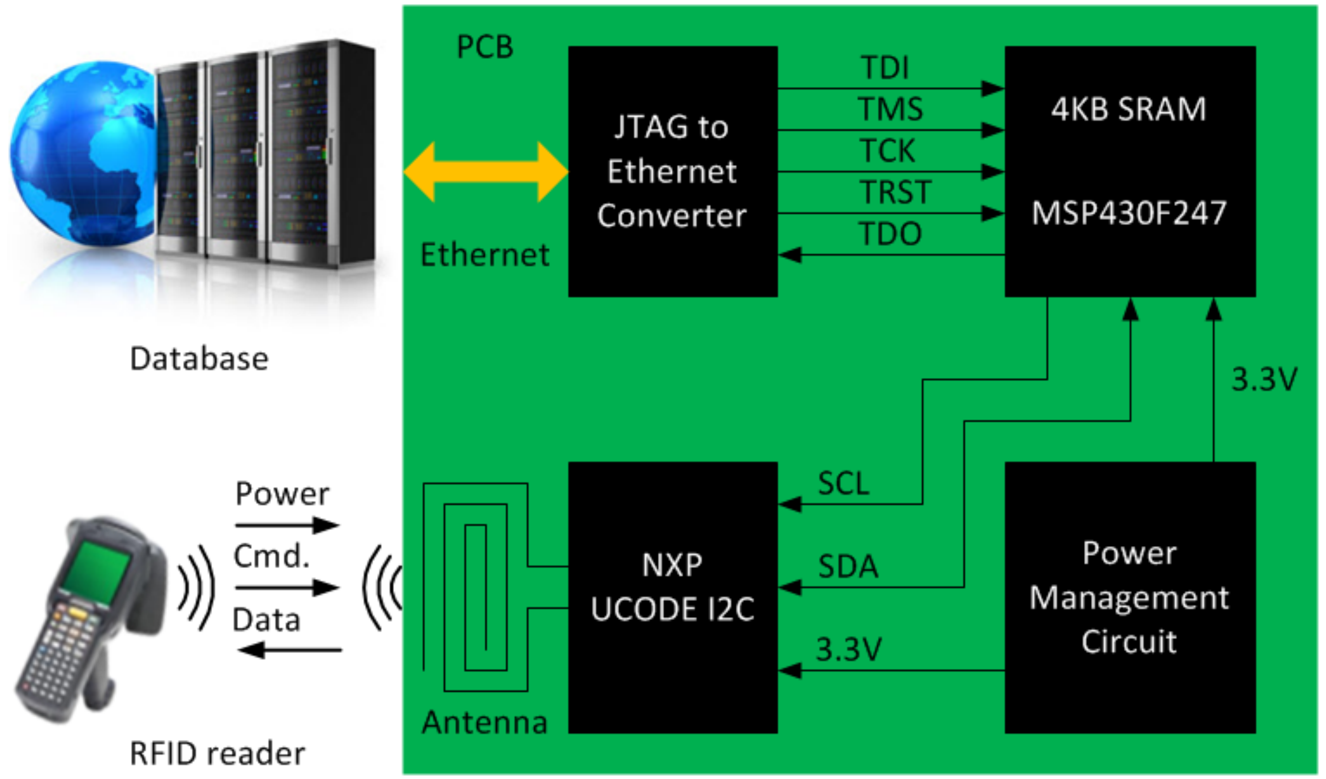


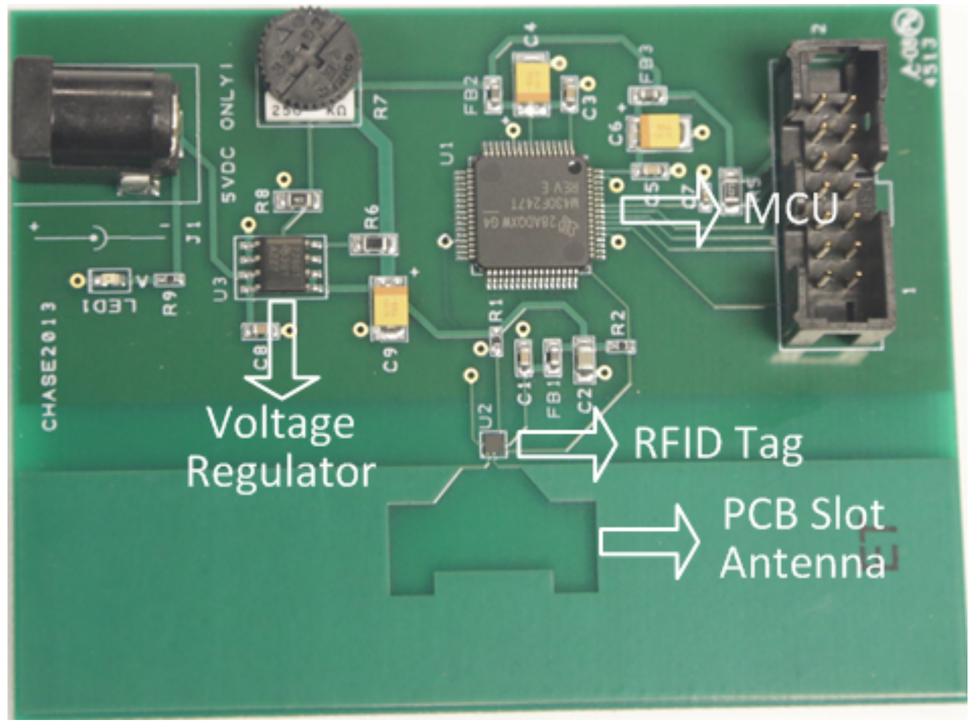
Supply Chain with Transition Points.

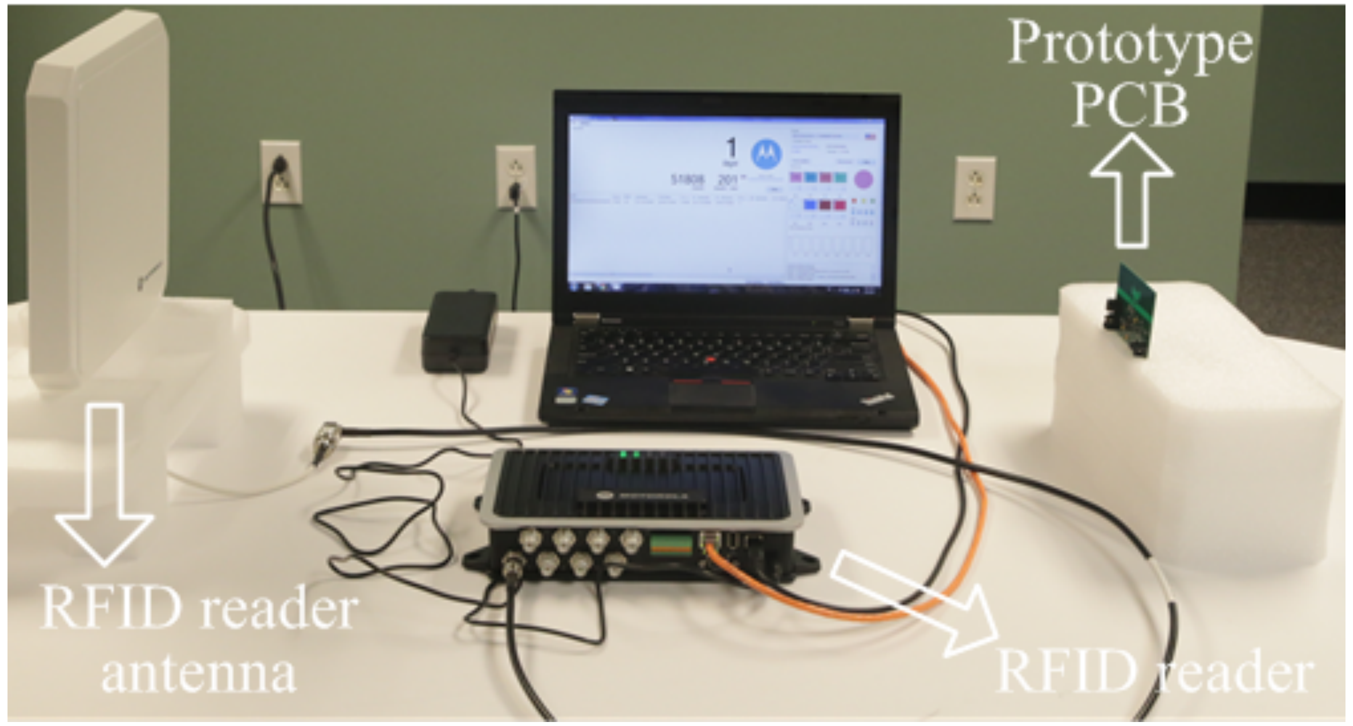


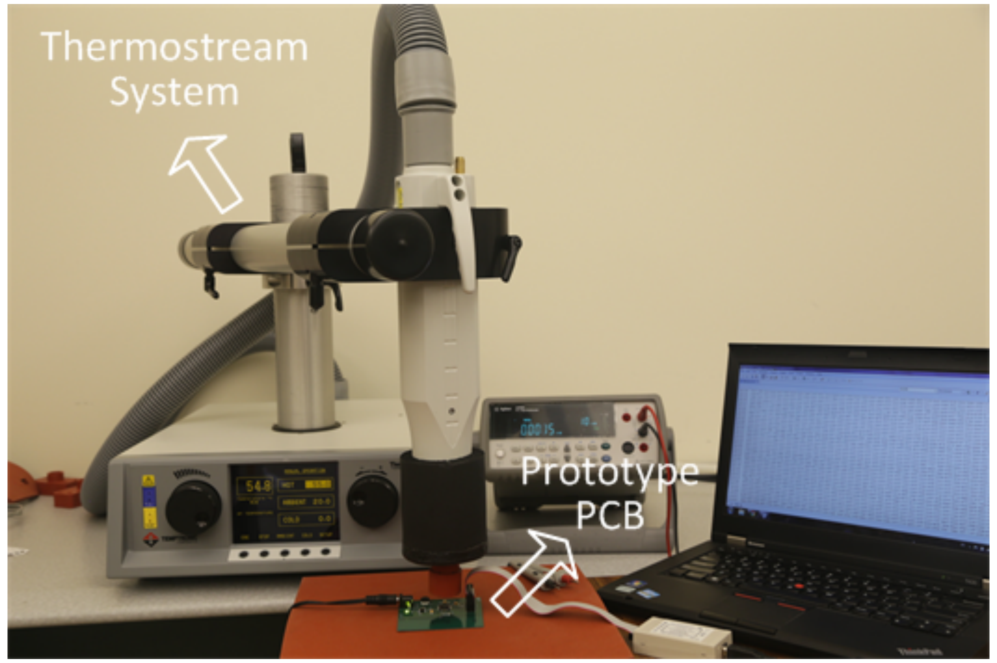
Attack Models.

Prototype


Database
RFID reader
Power
Cmd.
Data
PCB
Ethernet
JTAG to Ethernet Converter
TDI
TMS
TCK
TRST
TDO
4KB SRAM
MSP430F247
3.3V
SCL
SDA
3.3V
NXP UCODE I2C
Power Management Circuit
Antenna


MCU
Voltage Regulator
RFID Tag
PCB Slot Antenna

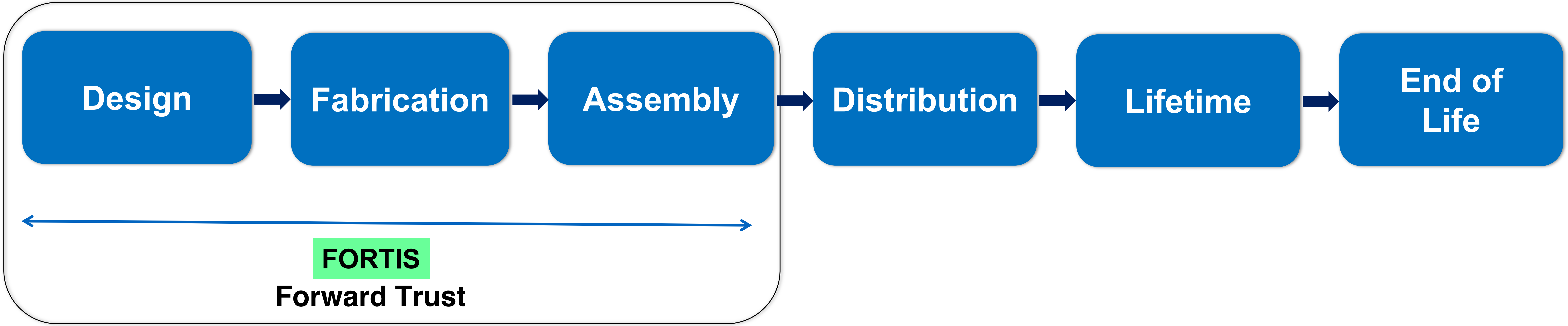

Prototype PCB
RFID reader antenna
RFID reader


Thermostream System
Prototype PCB

Outline

- Problem Statement and the Fundamentals
- Example Attacks
- Supply Chain Vulnerabilities
- PUF + ECID
- Counterfeit Electronics
- Logic Obfuscation / IP Encryption
- Hardware Trojans
- Research Challenges

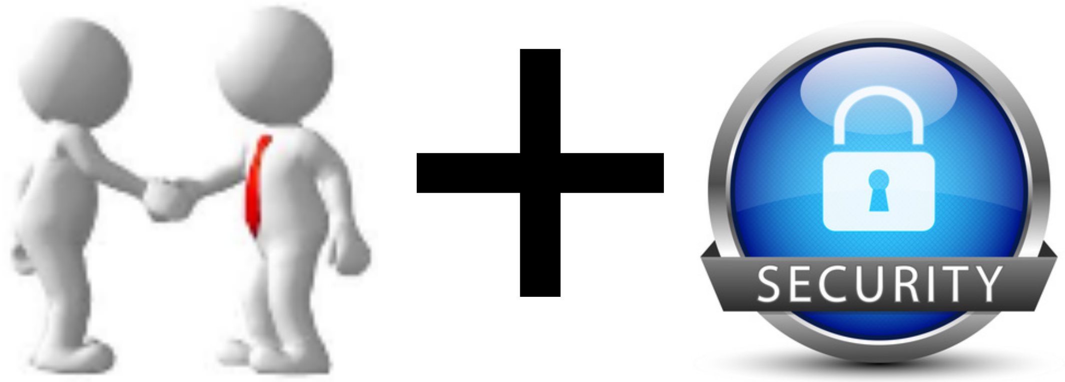
Protection Throughout the Lifecycle



Design → Fabrication → Assembly → Distribution → Lifetime → End of Life

FORTIS

Forward Trust



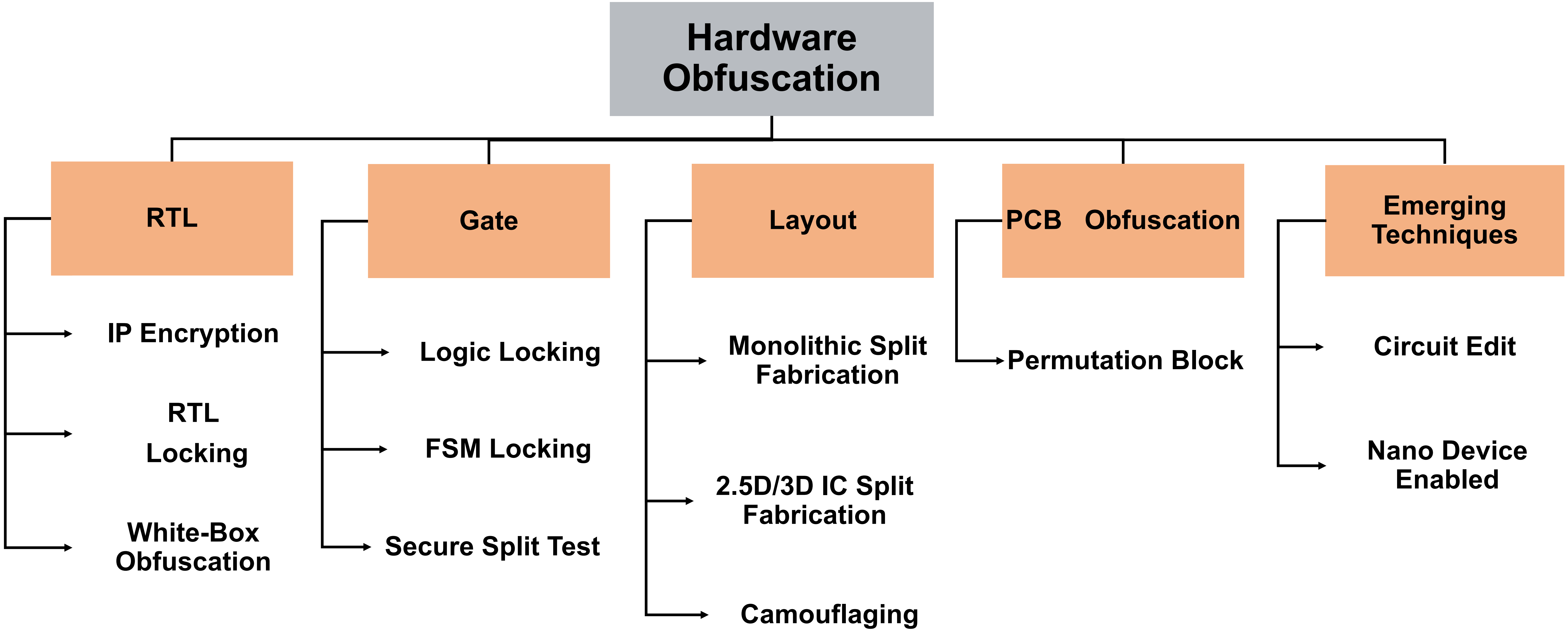
Hardware Obfuscation

- Techniques aimed at locking intellectual property and/or making it unintelligible for unauthorized parties

- Protects against
  - Overproduction: Prevents manufacturing of ICs/ICs with IPs beyond contracted amount by untrusted foundry
  - IP Piracy: Prevent unauthorized use of semiconductor intellectual property cores in designs
  - IC Piracy: Unauthorized use/reselling of manufactured ICs by untrusted foundry
  - Trojan insertion: Prevents malicious tampering of design as functionality is obfuscated

- Can be applied at several abstraction levels of the design
  - Register Transfer Level (RTL)
  - Gate Level
  - Layout / Level

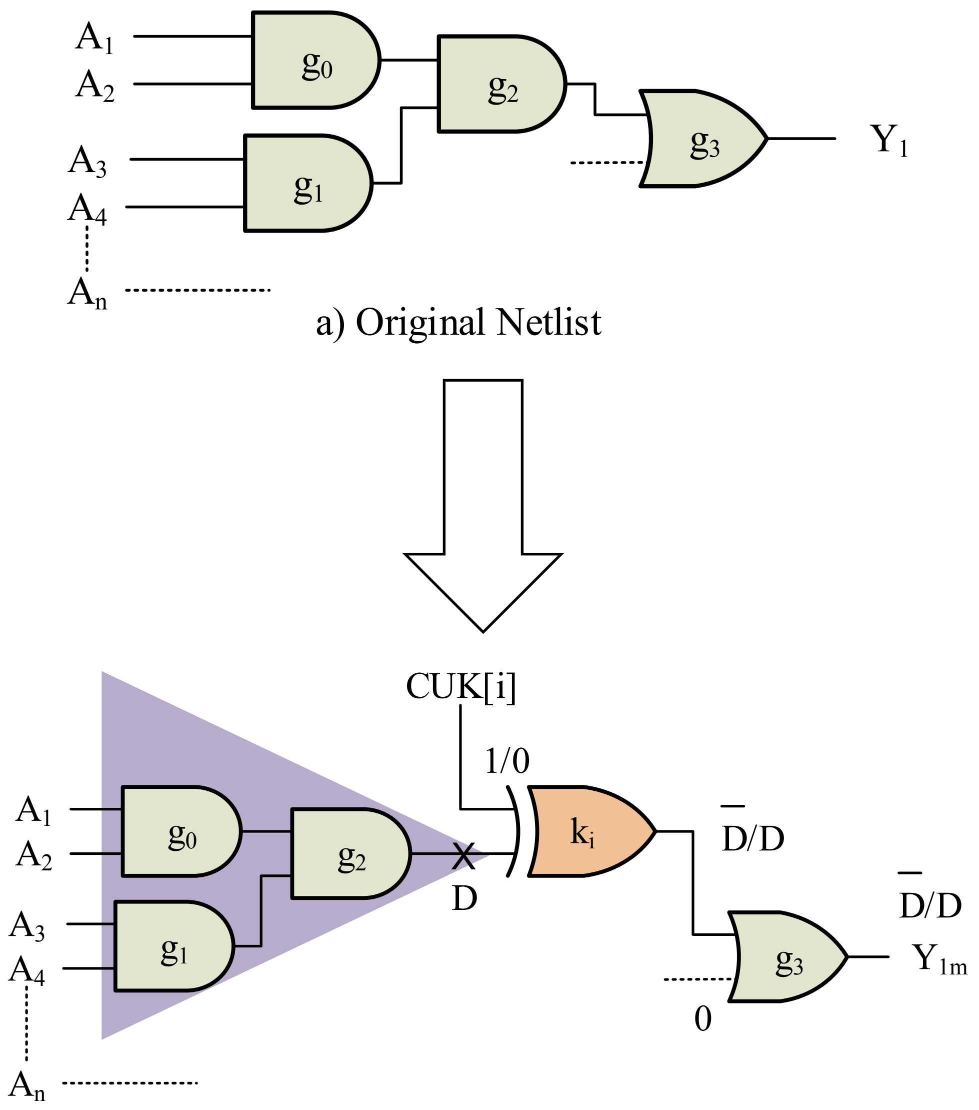
Taxonomy of Hardware Obfuscation Approaches



Hardware Obfuscation

- RTL
  - IP Encryption
  - RTL Locking
  - White-Box Obfuscation
- Gate
  - Logic Locking
  - FSM Locking
  - Secure Split Test
- Layout
  - Monolithic Split Fabrication
  - 2.5D/3D IC Split Fabrication
  - Camouflaging
- PCB Obfuscation
  - Permutation Block
- Emerging Techniques
  - Circuit Edit
  - Nano Device Enabled

Gate-Level Logic Encryption



a) Original Netlist

b) Obfuscated netlist

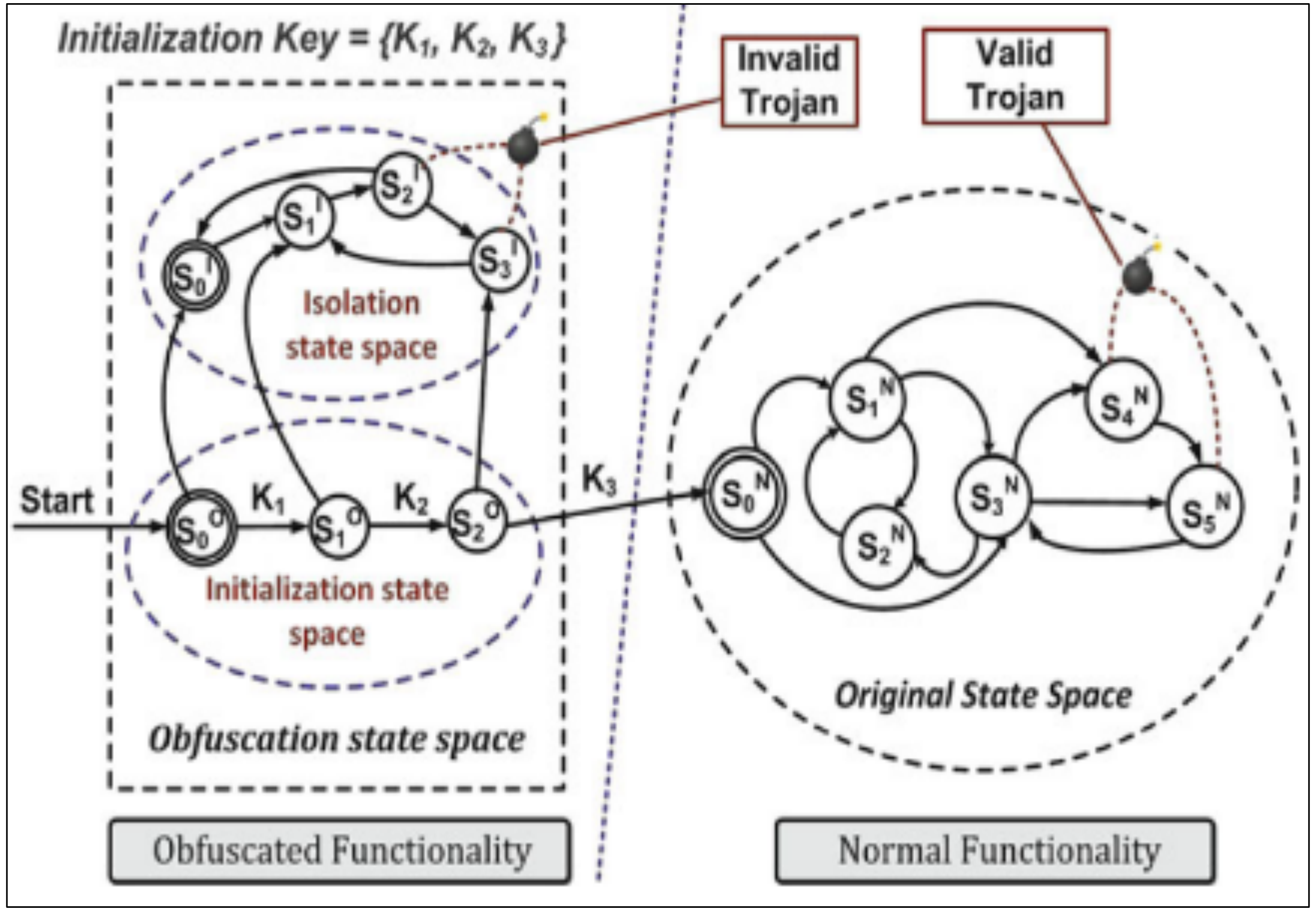
CUK: Chip Unlocking Key

- Most popular proposed method for locking design at gate-level
- Additional key gates inserted into design netlist (XOR, XNOR, MUX, AND, OR, LUTs etc.)
- Design fails to produce correct I/O behavior *unless* correct key is provided to key gates
- Various techniques for insertion

1. Random insertion
2. Fault analysis: Insert key gates at observable locations
3. Interference: Prevent propagation of key values to output
4. SAT resistance: Limit resistance to satisfiability based attacks
5. Logic barrier: Every path from input to output goes through key gates

Logic Obfuscation – FSM based Approach

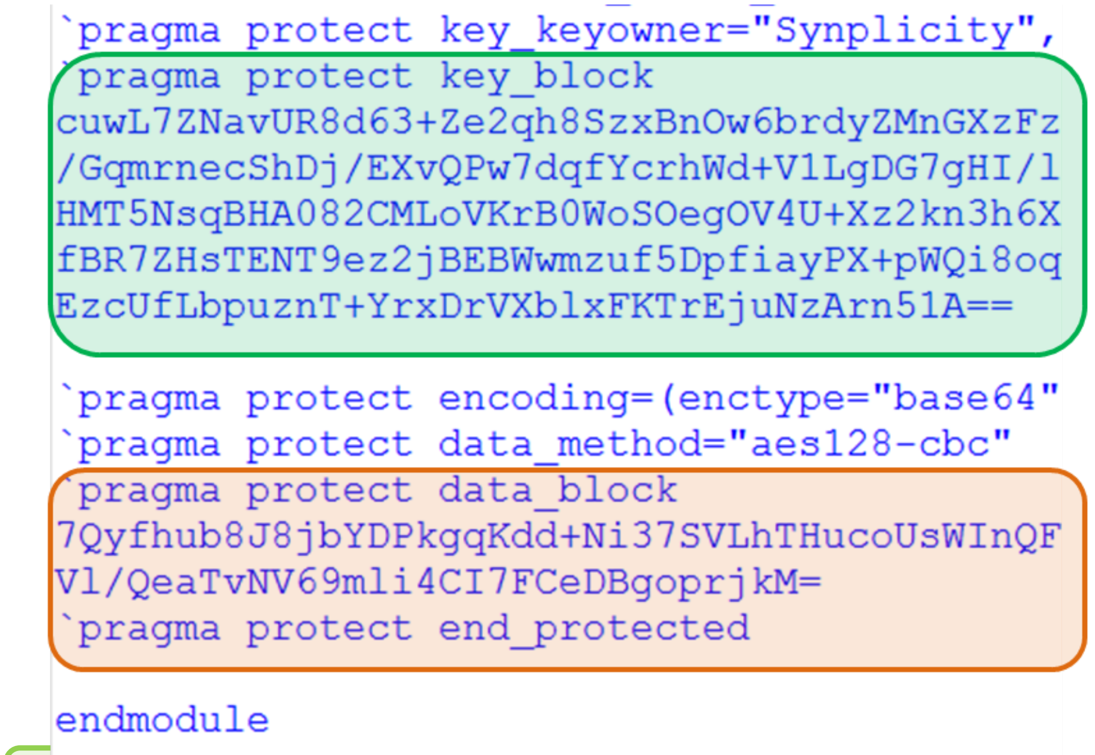
- Add an obfuscated mode on top of the original transition functionality.
- Obfuscation pattern guides the circuit to normal mode.
- Transition arc K3 offers the sole design route from obfuscated mode to normal mode
- Obfuscation also protects original functionality – prevents IP Piracy from an untrusted foundry



Bhunia, et. al., “HARPOON: an obfuscation-based SoC design methodology for hardware protection,” TCAD 2009.

IEEE P1735

- IEEE standard for IP encryption → Prevent **IP piracy**
  - Primary purpose → **Protect confidentiality and integrity**
  - Rights management → Control IP visibility
  - Supports licensing → Restrict access to particular IP users
  - Digest → Prevents tampering with **key block**



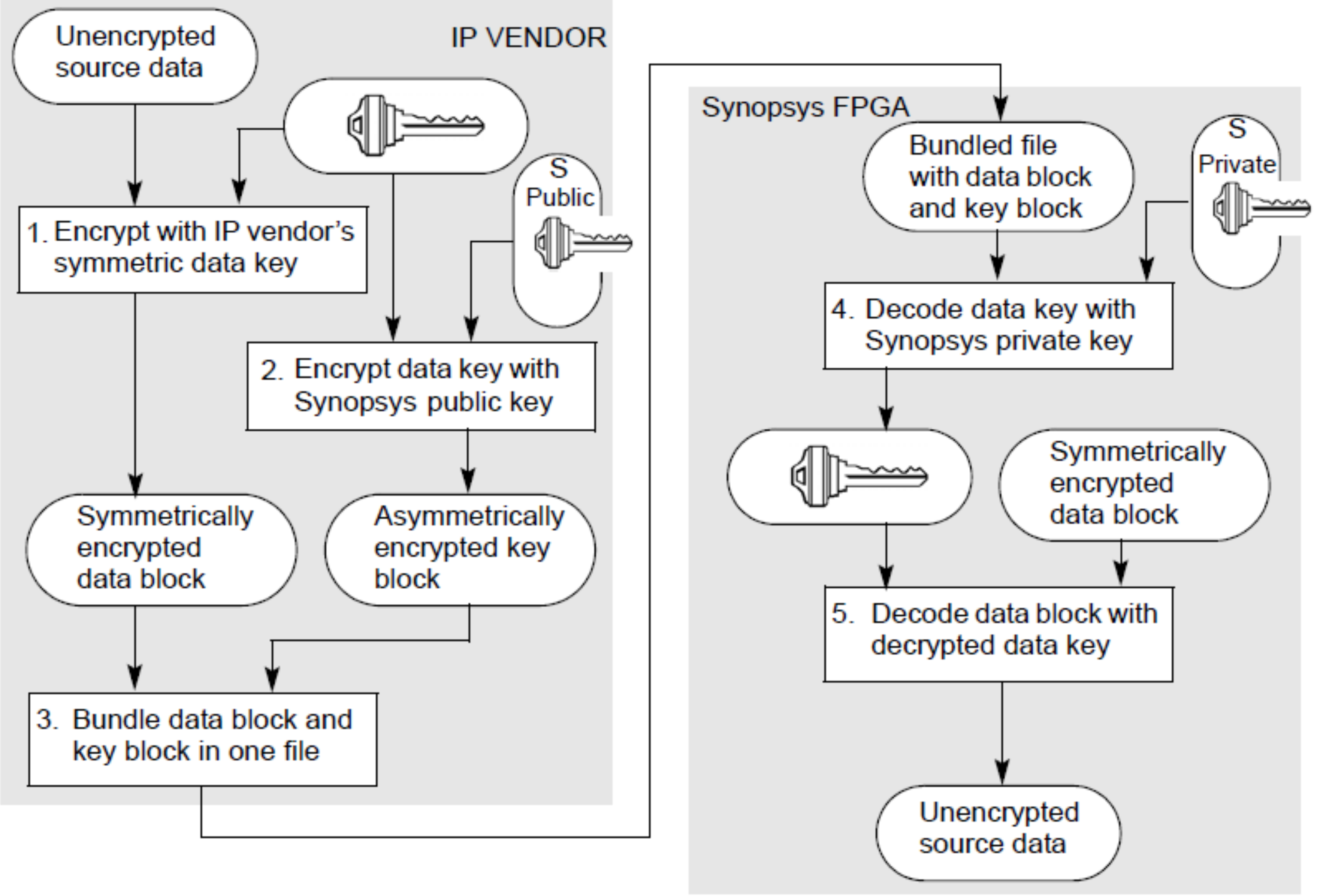
```
`pragma protect key_keyowner="Synplicity",
`pragma protect key_block
cuwL7ZNavUR8d63+Ze2qh8SzxBnOw6brdyZMnGXzFz
/GqmrnecShDj/EXvQPw7dqfYcrhWd+V1LgDG7gHI/l
HMT5NsqBHA082CMLoVKrB0WoSOegOV4U+Xz2kn3h6X
fBR7ZHsTENT9ez2jBEBWwmzuf5DpfiayPX+pWQi8oq
EzcUfLbpuznT+YrxDrVXblxFKTrEjuNzArn51A==

`pragma protect encoding=(enctype="base64"
`pragma protect data_method="aes128-cbc"
`pragma protect data_block
7QyfhubJ8jbYDPkgqKdd+Ni37SVLhTHucoUsWInQF
Vl/QeaTvNV69mli4CI7FCeDBgoprjkM=
`pragma protect end_protected

endmodule
```

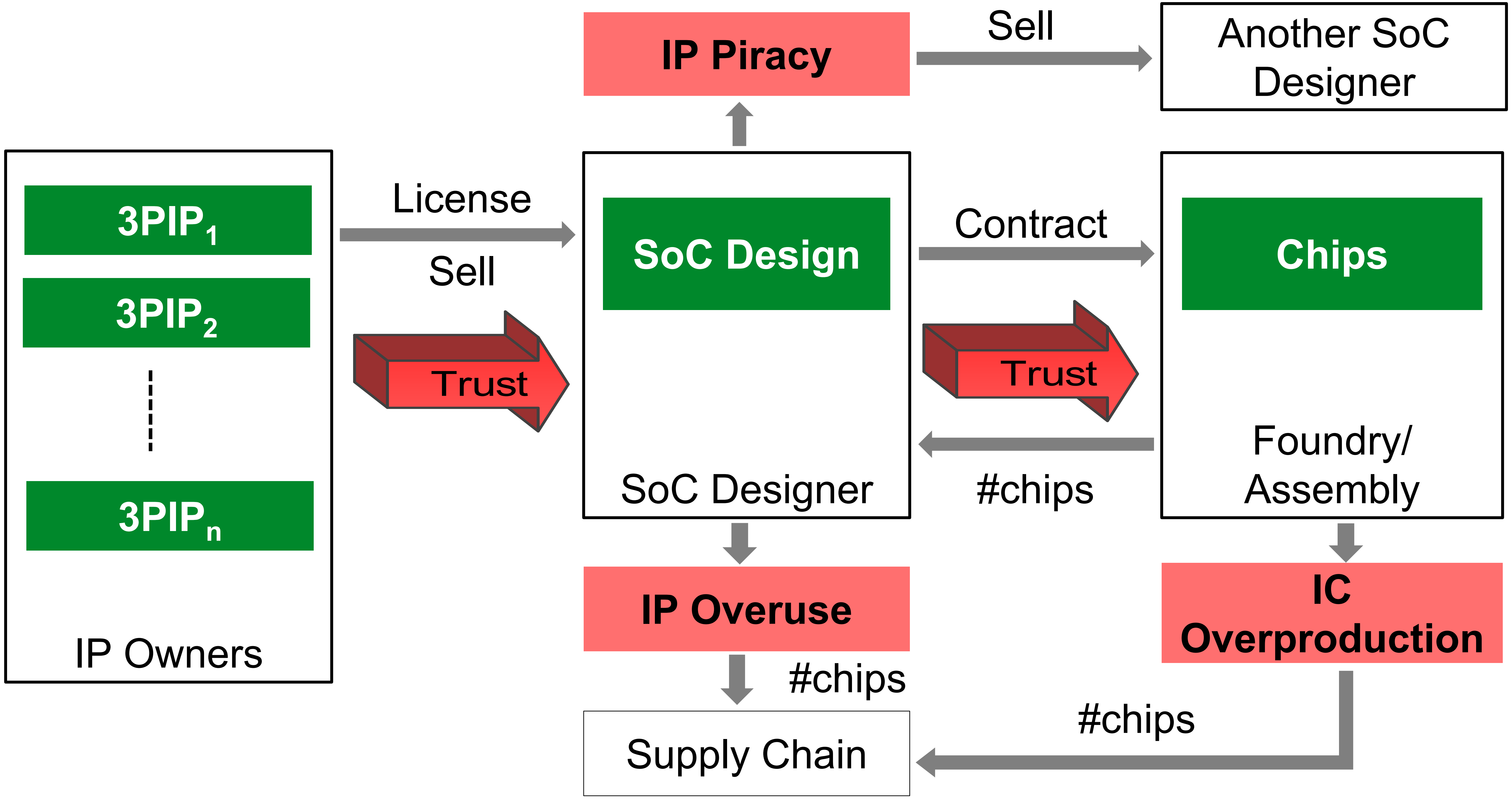
🟩 Key Block → Session key

🟧 Data Block → Encrypted RTL code

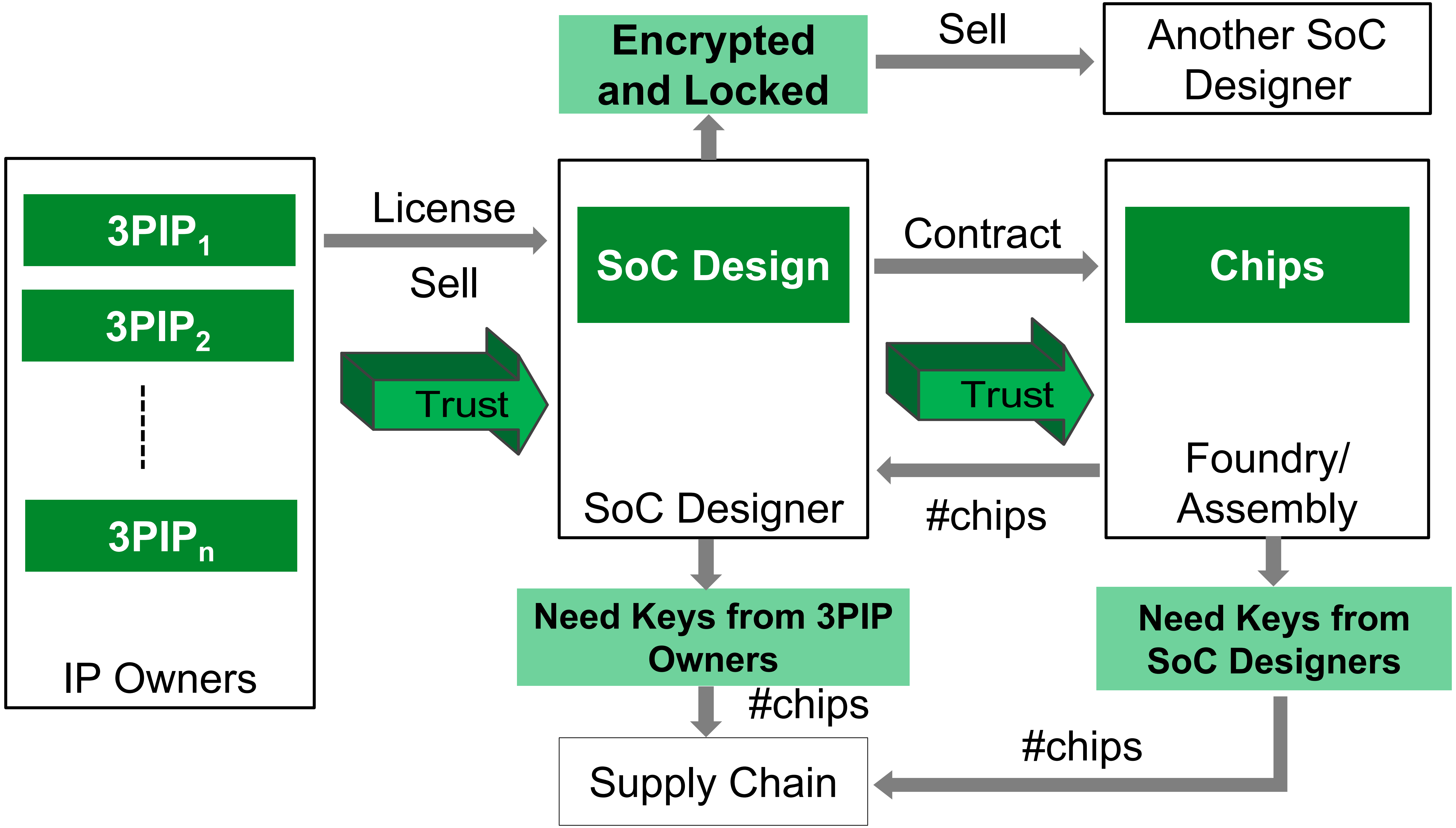


IP VENDOR
Unencrypted source data
1. Encrypt with IP vendor's symmetric data key
S
Public
2. Encrypt data key with Synopsys public key
Symmetrically encrypted data block
Asymmetrically encrypted key block
3. Bundle data block and key block in one file
Synopsys FPGA
Bundled file with data block and key block
S
Private
4. Decode data key with Synopsys private key
Symmetrically encrypted data block
5. Decode data block with decrypted data key
Unencrypted source data

Design-to-Fab Trust Risk

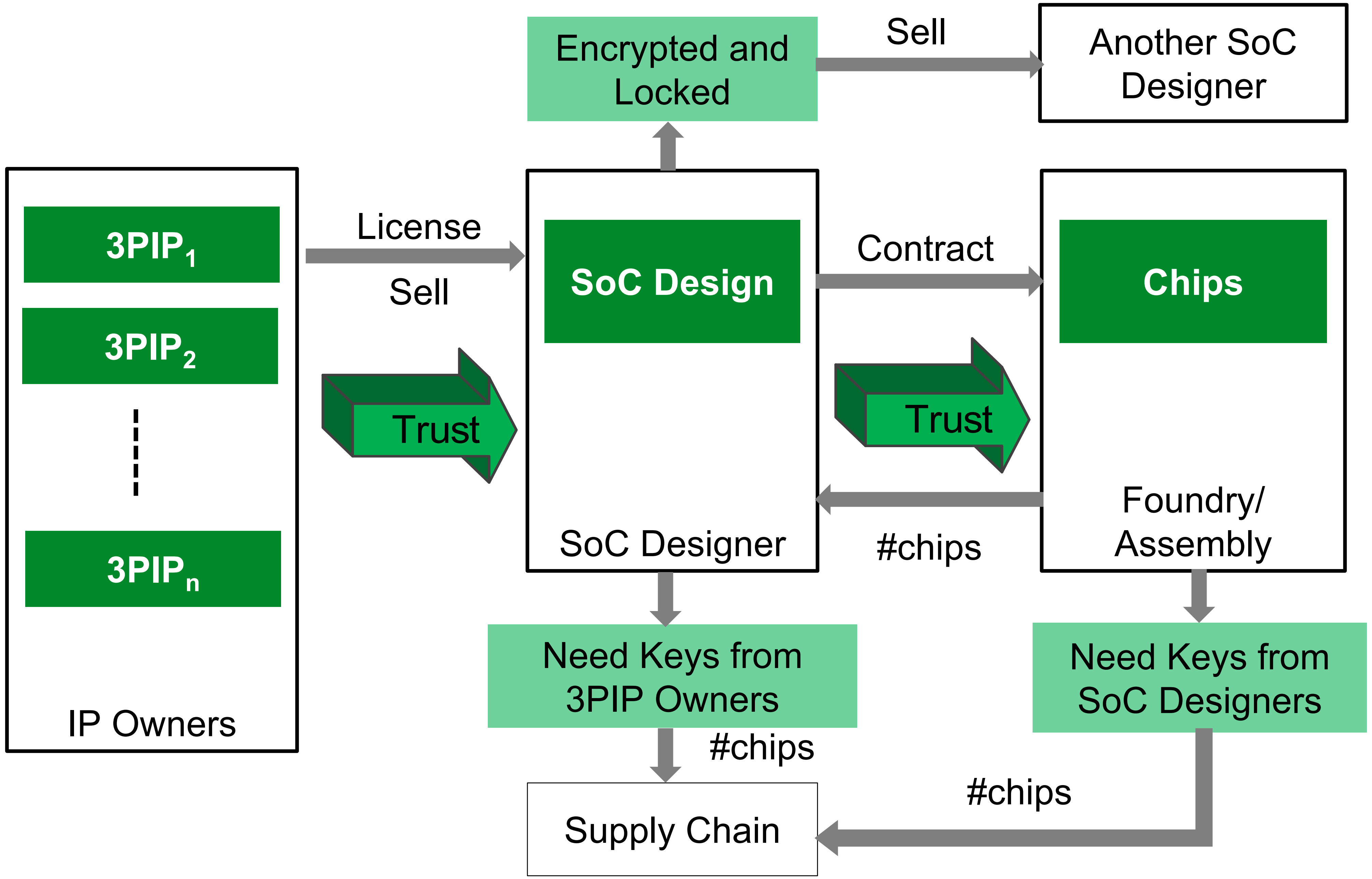


Establishing Forward Trust

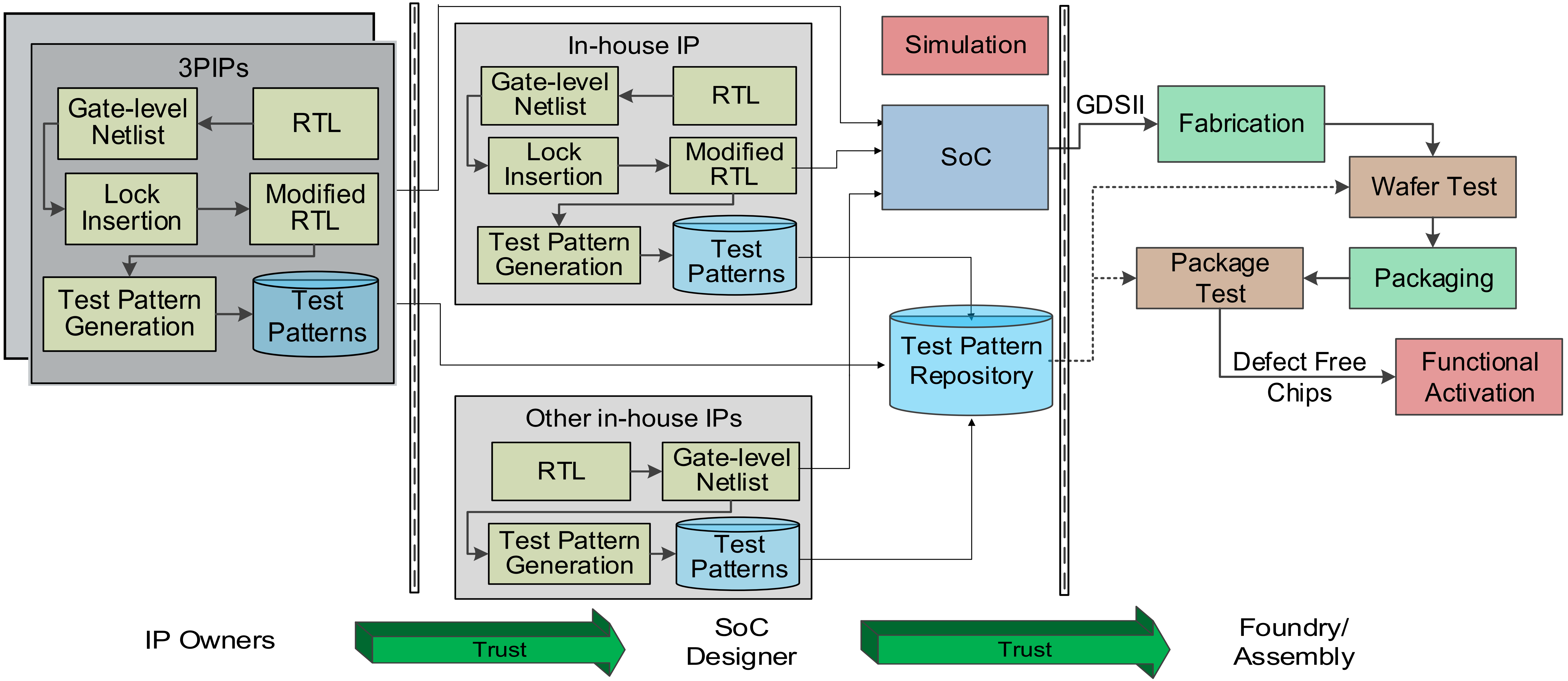


Challenges

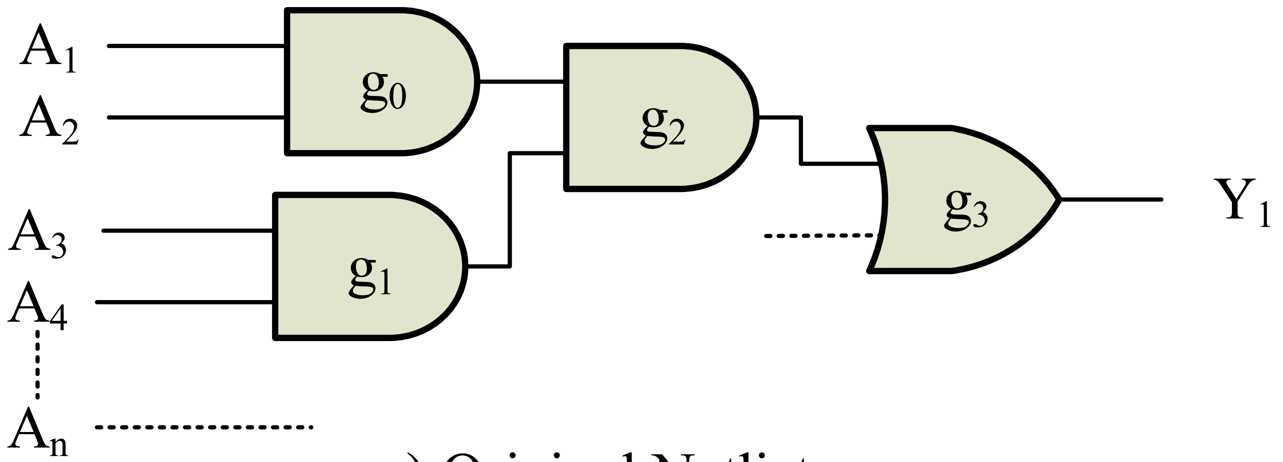
- How to lock a netlist which activates test before unlocking?
- How to securely transfer the keys from 3PIP owners and SoC designer to the foundry and assembly?
- How to protect a 3PIP from unwanted modification?



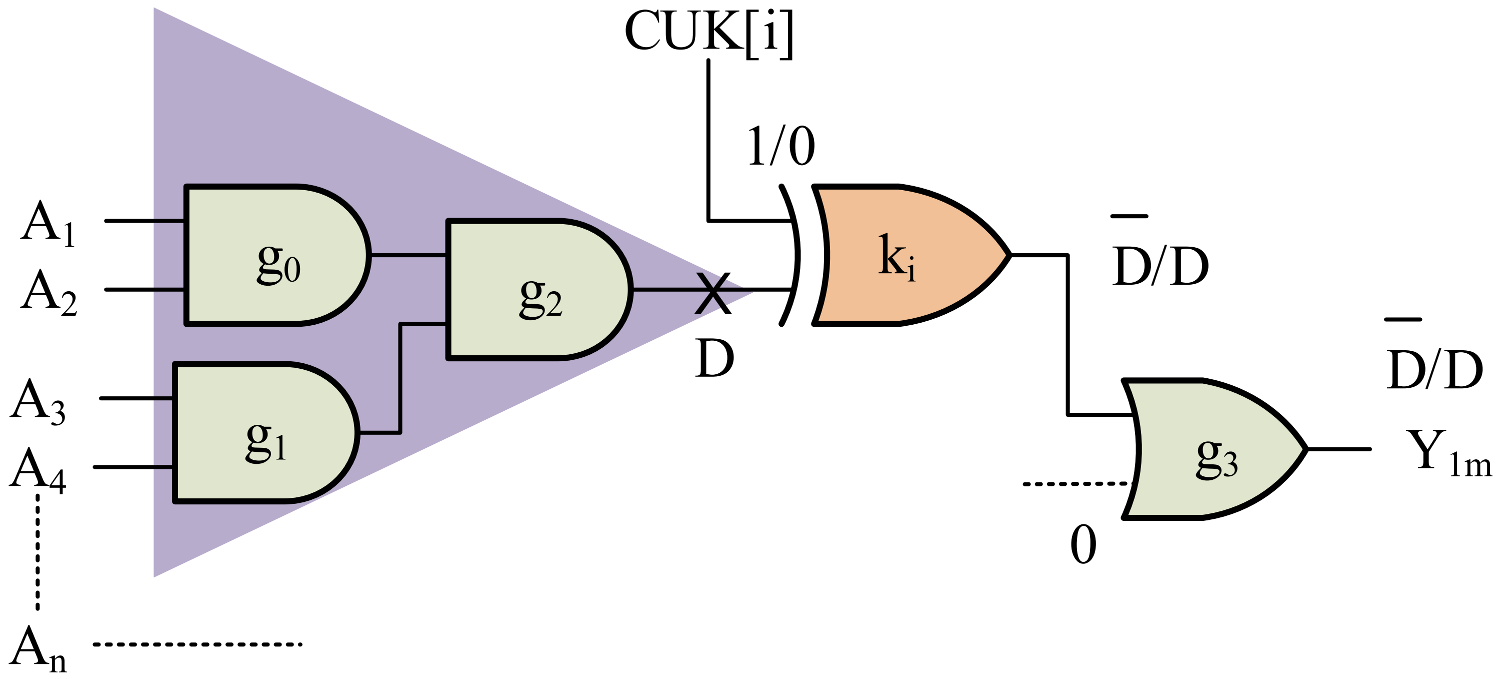
FORTIS -- Framework



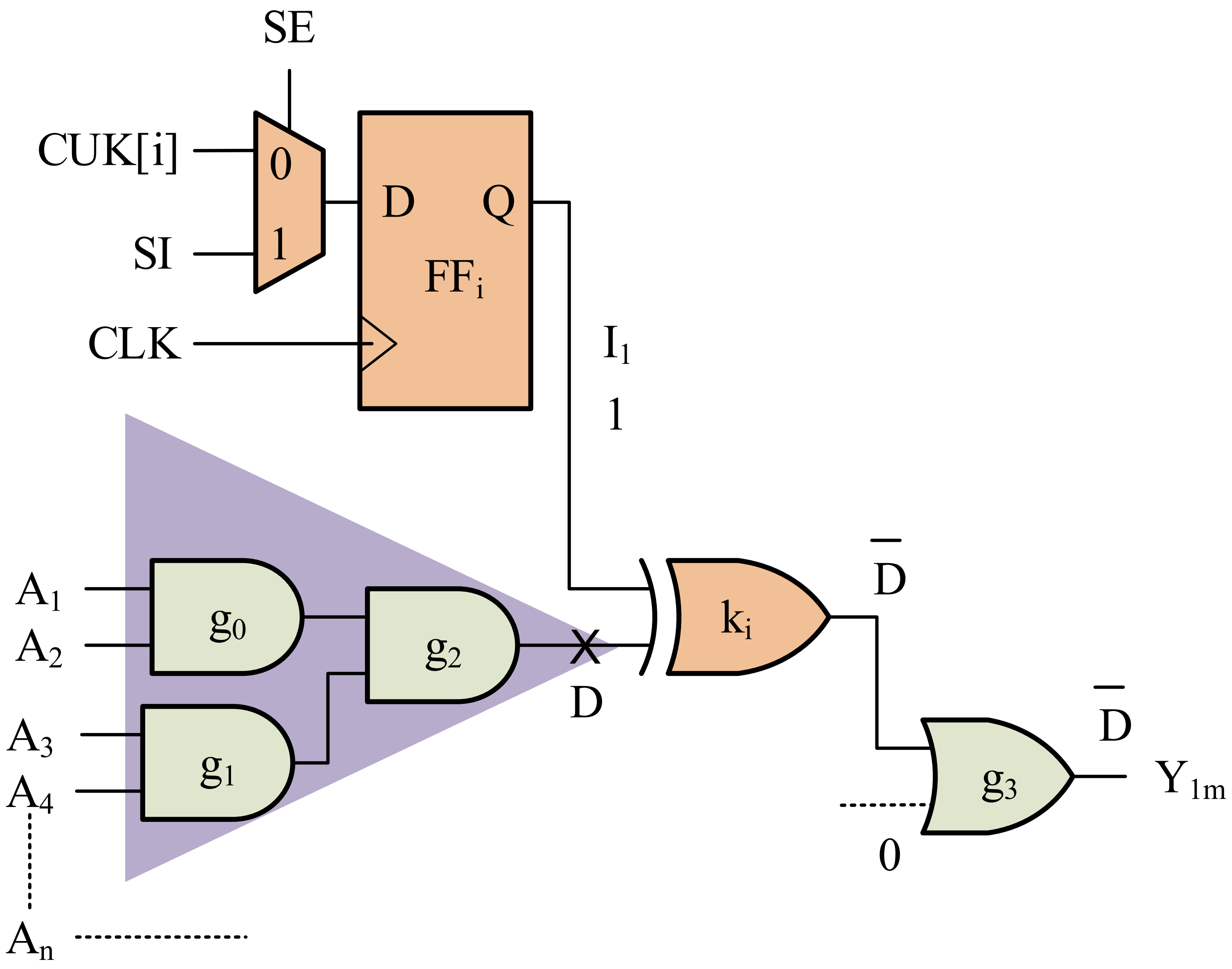
Test Before IC Activation



a) Original Netlist



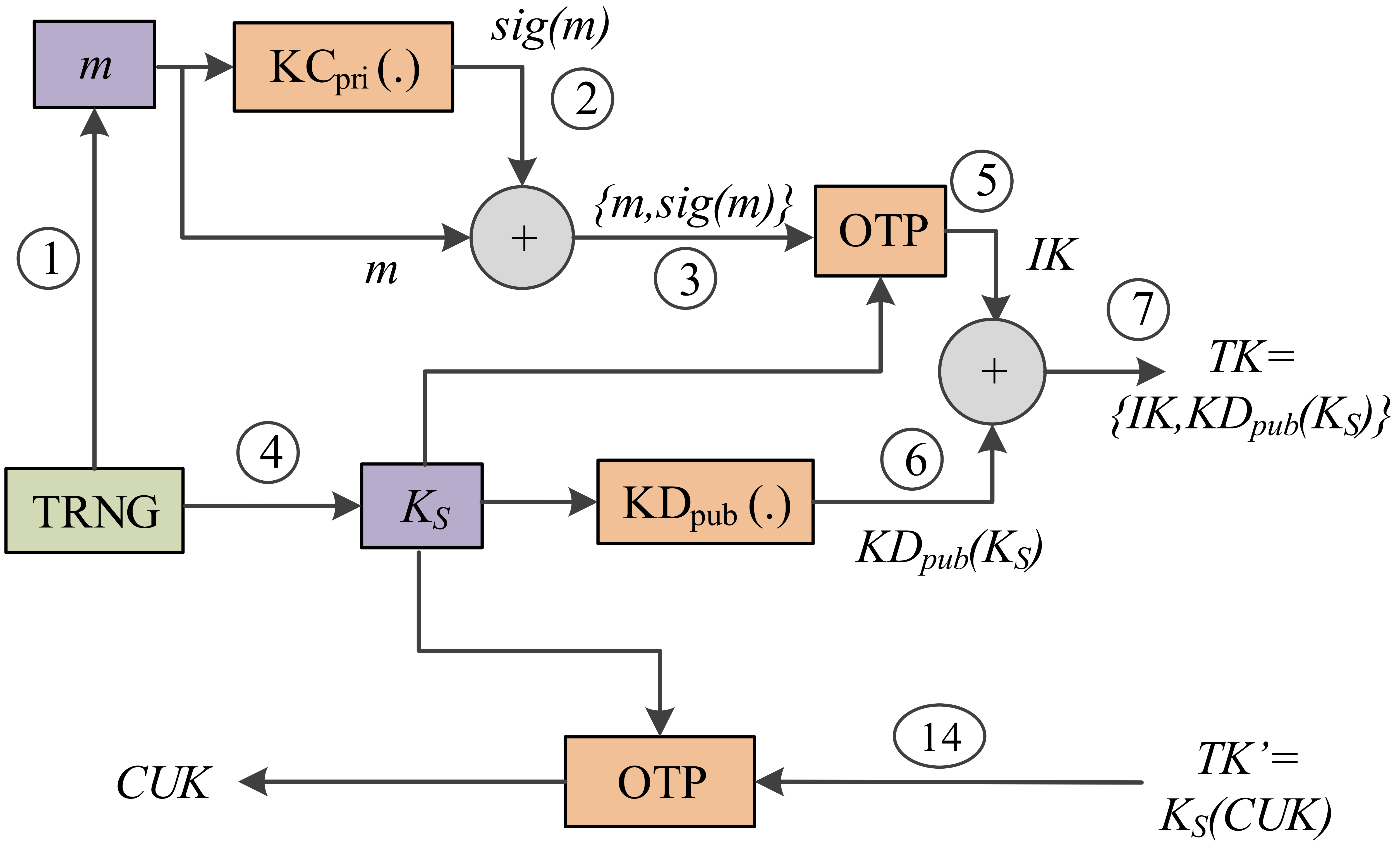
b) Obfuscated netlist



c) Proposed Netlist

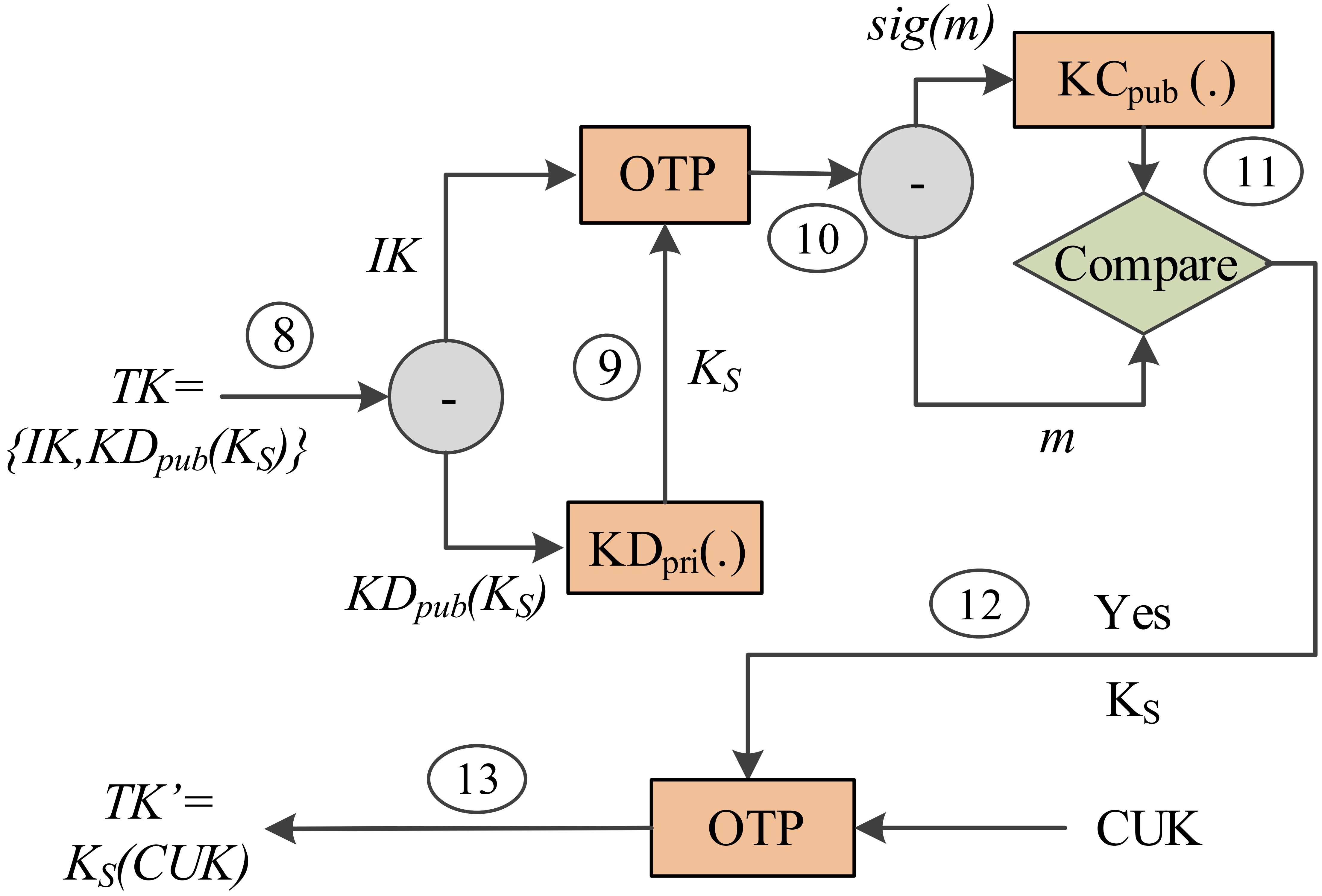
Key Transfer: Chip Side

System on a Chip

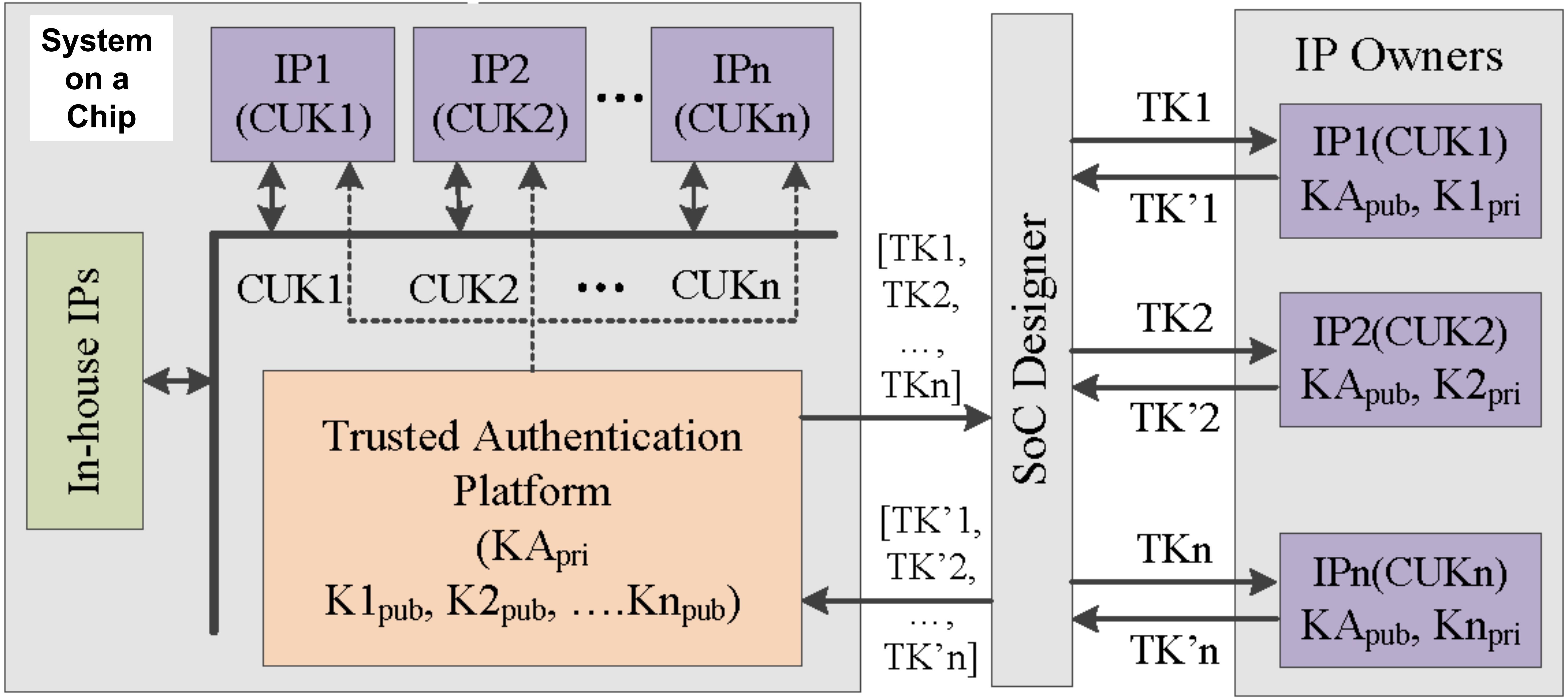


Key Transfer: SoC Designer Side

System on a Chip Designer



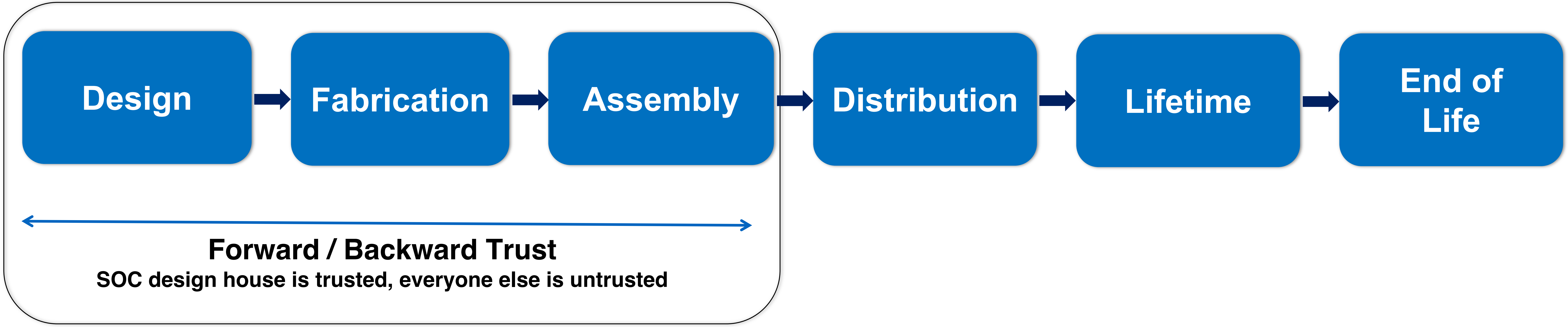
IP Overuse


System on a Chip
IP1 (CUK1)
IP2 (CUK2)
...
IPn (CUKn)
In-house IPs
CUK1
CUK2
...
CUKn
Trusted Authentication Platform (KA_{pri} $K1_{pub}$, $K2_{pub}$, ...Kn_{pub})
[TK1, TK2, ..., TKn]
[TK'1, TK'2, ..., TK'n]
SoC Designer
TK1
TK'1
TK2
TK'2
TKn
TK'n
IP Owners
IP1(CUK1) KA_{pub}, $K1_{pri}$
IP2(CUK2) KA_{pub}, $K2_{pri}$
IPn(CUKn) KA_{pub}, Kn_{pri}

Outline

- Problem Statement and the Fundamentals
- Example Attacks
- Supply Chain Vulnerabilities
- PUF + ECID
- Counterfeit Electronics
- Logic Obfuscation / IP Encryption
- Hardware Trojans
- Research Challenges

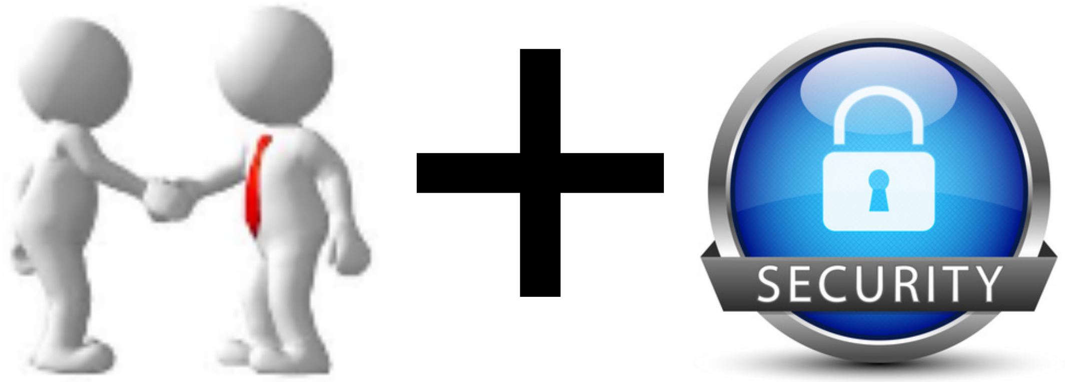
Protection Throughout the Lifecycle



Design → Fabrication → Assembly → Distribution → Lifetime → End of Life

Forward / Backward Trust

SOC design house is trusted, everyone else is untrusted



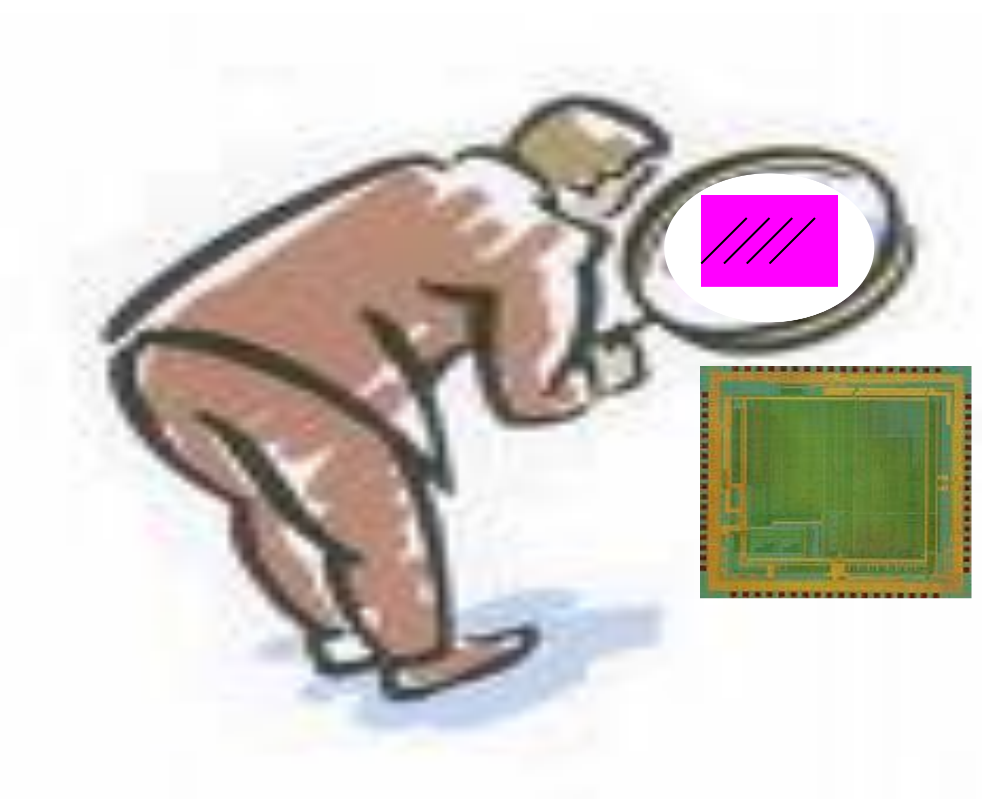
IP Trust

- IPs from untrusted vendors need to be verified for trust before use in a system design
- How can one establish that the IP does exactly as the specification, nothing less nothing more?
- IP cores: soft IP, firm IP and hard IP
- Challenges:
  - No known golden model for the IP as that for IC
  - Soft IP is just a code so that we cannot read its implementation
  - No side-channel information

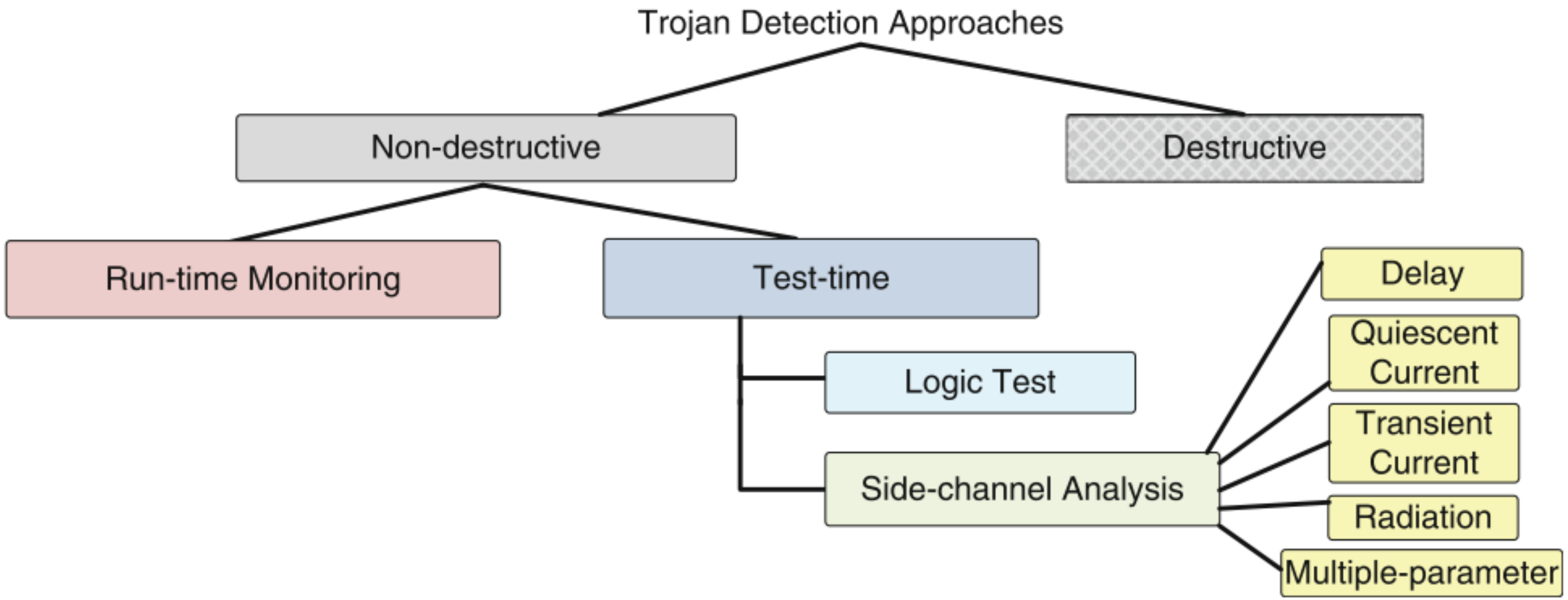
IC Trust

- **The objective is to ensure that the fabricated chip/system will carry out only our desired function and <u>nothing more</u>.**

- **Challenges:**
  - Tiny: several gates to millions of gates
  - Quiet: hard-to-activate (rare event) or triggered itself (time-bomb)
  - Hard to model: human intelligence
  - Conventional test and validation approaches fail to reliably detect hardware Trojans.
    - Focus on manufacture defects and does not target detection of additiona functionality in a design



Classification of Trojan Detection Approaches



- **Destructive Approach: expensive and time consuming**
  - Reverse engineering to extract layer-by-layer images by using Scanning Electron Microscope
  - Identify transistors or gates and routing elements by using a template-matching approach

Logic Testing Approach

- **Logic-testing approach focuses on test-vector generation for**
  - Activating a Trojan circuit
  - Observing its malicious effect on the payload at the primary outputs
  - Both functional and structural test vectors are applicable.

- **Pros & Cons:**
  - Pros: straight-forward and easy to differentiate
  - Cons:
    - The difficulty in exciting or observing low controllability or low observability nodes.
    - Intentionally inserted Trojans are triggered under rare conditions.
      (e.g., sequential Trojans)
    - It cannot trigger Trojans that are activated externally and can only observe functional Trojans.

Side-Channel Analysis-Based Approaches

- **All the side-channel analyses are based on observing the effect of an inserted Trojan on a physical parameter such as**
  - IDDQ: Extra gates will consume leakage power.
  - IDDT: Extra switching activities will consume more dynamic power.
  - Path delay: Additional gates and capacitance will increase path delay.
  - EM: Electromagnetic radiation due to switching activity

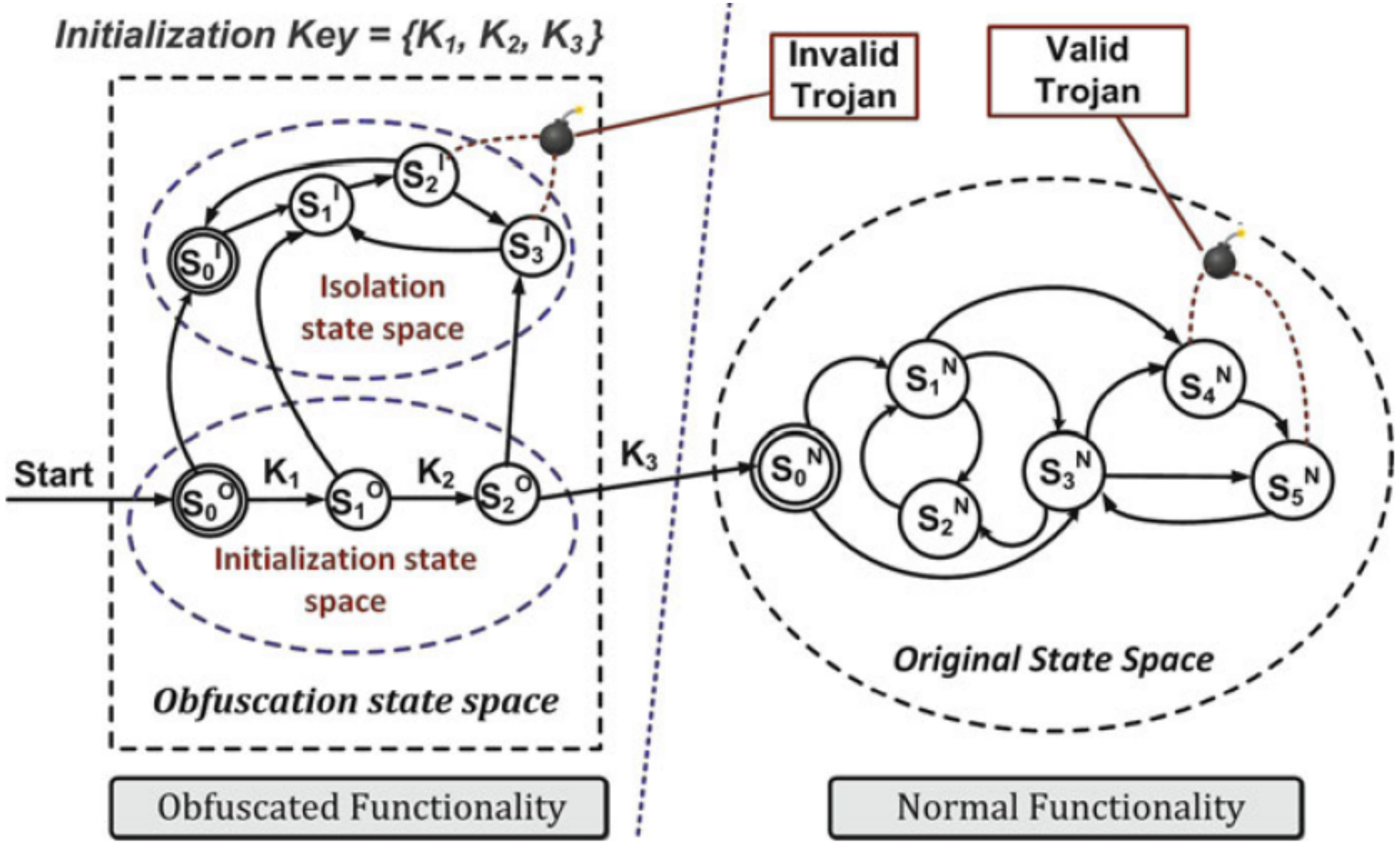
- **Pros & Cons**
  - Pros: It is effective for Trojan which does not cause observable malfunction in the circuits.
  - Cons: Large process variations in modern nanometer technologies and measurement noise can mask the effect of the Trojan circuits, especially for small Trojan.

Design for Hardware Trust

- **Since detecting Trojan is extremely challenging, design for hardware trust approaches are proposed to**
  - **Improve hardware Trojan detection methods**
    - Improve sensitive to power and delay
    - Rare event removal
  - **Prevent hardware Trojan insertion**
    - Design obfuscation
    - BISA

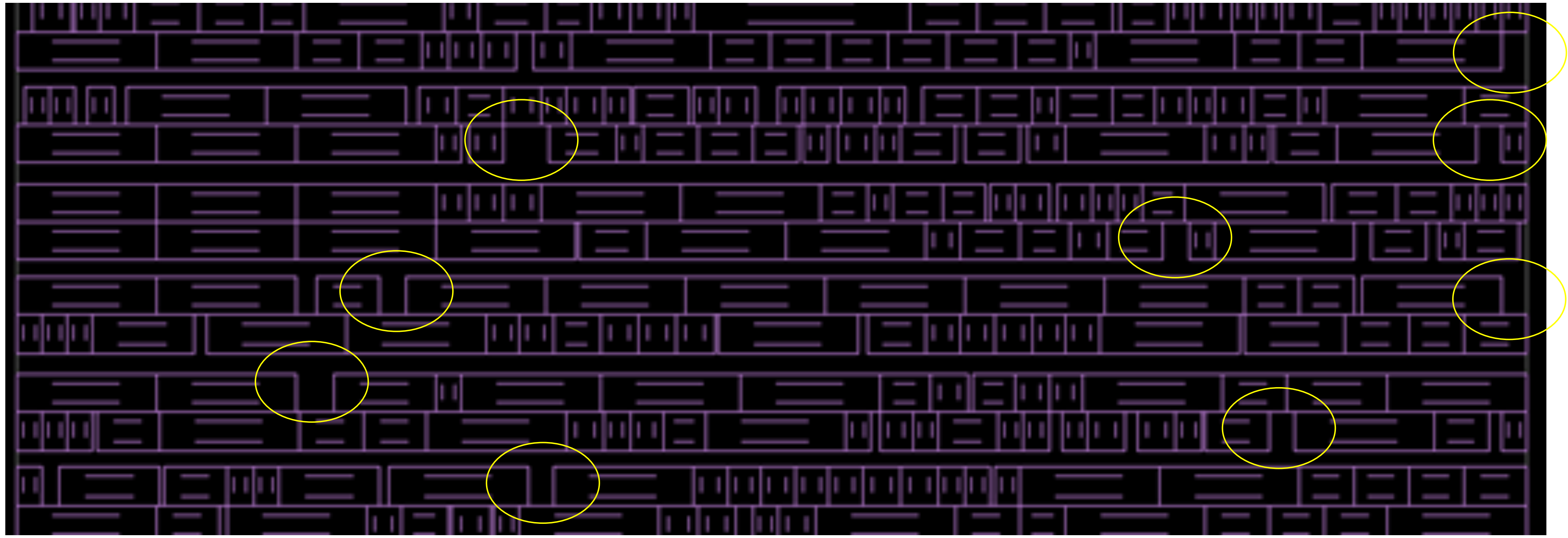
Logic obfuscation

- Specified pattern is able to guide the circuit into its normal mode.
- The transition arc K3 is the only way the design can enter normal operation mode from the obfuscated mode.



Prevention

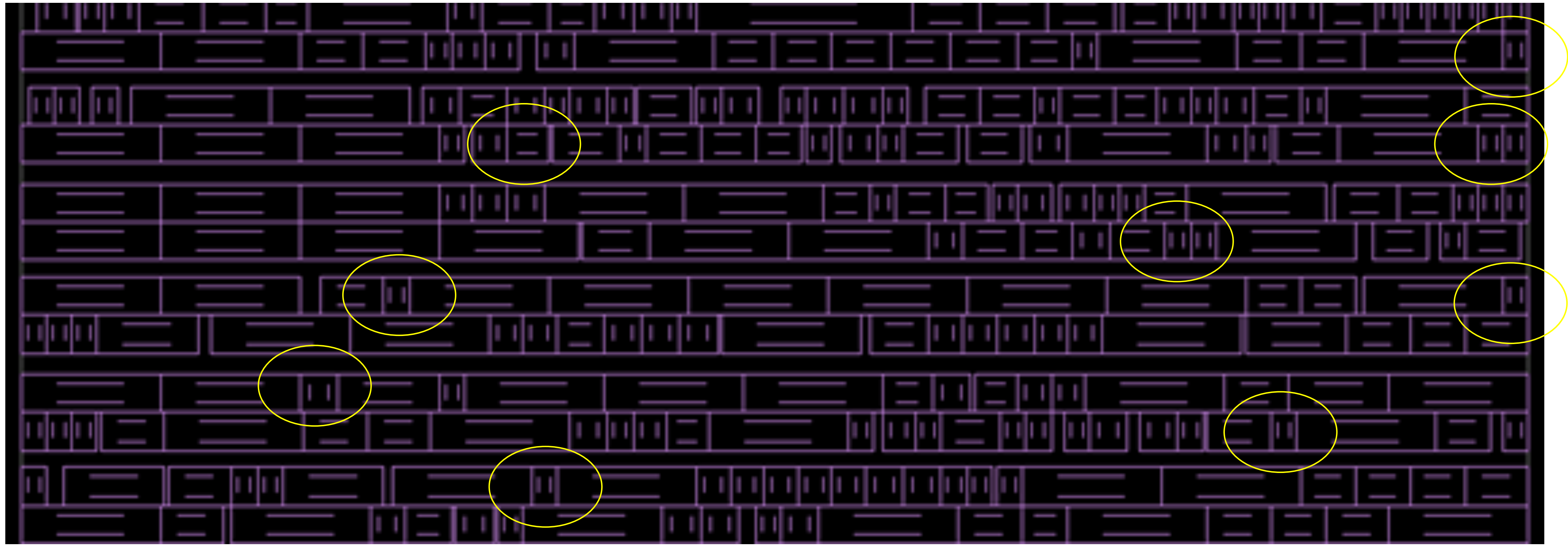
- ➢ Floorplanning tools typically are conservative to limit the density of cells in order to assure routability.
  - This often leaves small gaps between cells, and it is impossible to fill 100% of the area with standard cells in VLSI designs.



- ➢ Unused spaces will be filled with filler cells or decoupling capacitor cells in order to reduce the design rule check (DRC) violations created by the case layers and to ensure power rail connection.

BISA: Built-In Self-Authentication

- All hardware Trojans (except parametric Trojan) need extra gates for Trojan triggers and payloads to perform particular malicious behaviors.
- Since these inserted filler cells don’t have functionality, attackers can easily identify them and remove them to create space for their Trojan gates.
- Thus, we propose a Trojan-insertion prevention technique, called built-in self-authentication (BISA), to effectively handle these unused spaces in the layout.

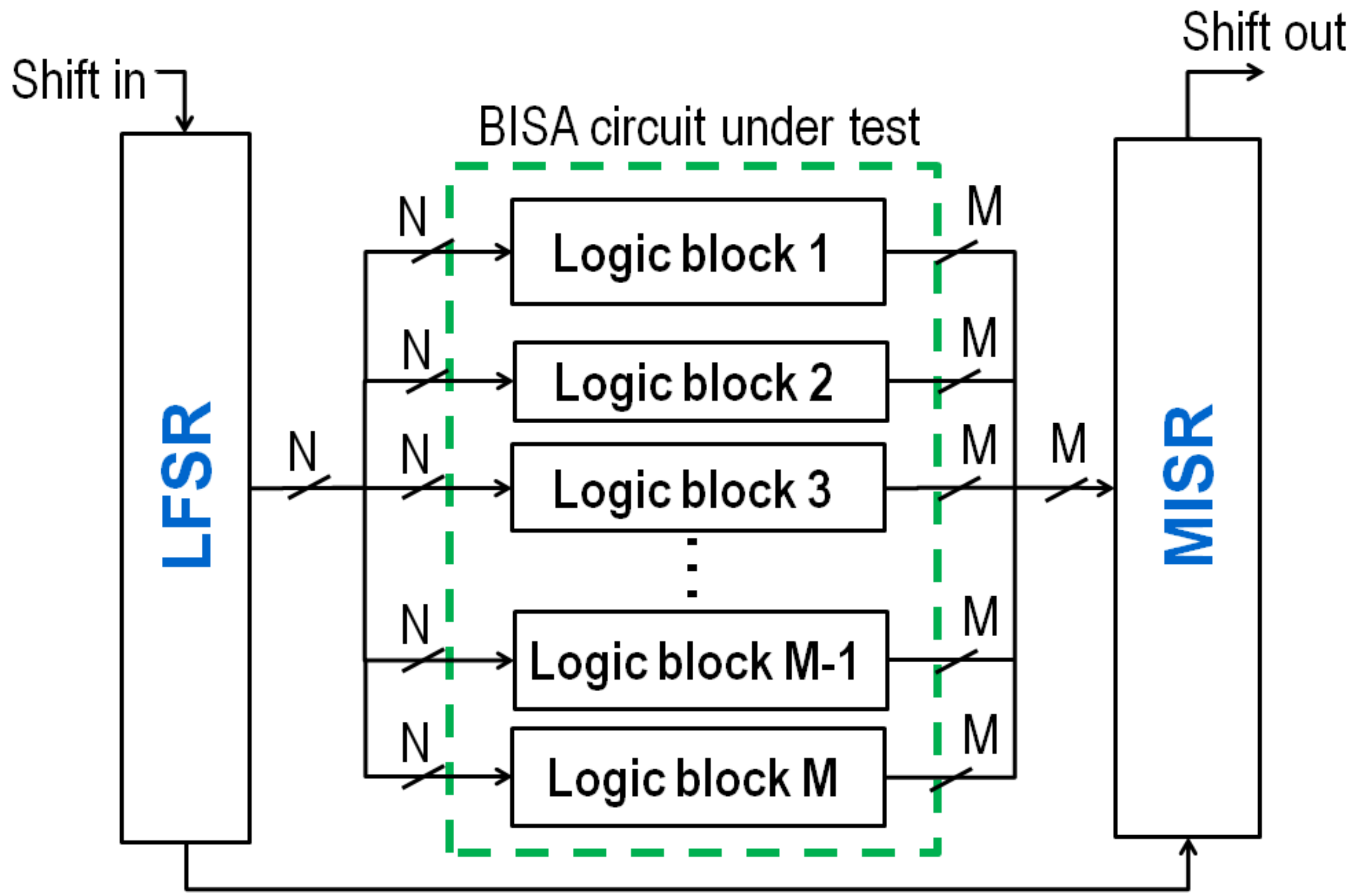


BISA: Built-In Self-Authentication

- BISA can fill unused spaces in a circuit layout with functional standard cell (BISA cell) instead of conventional non-functional filler cells.
- Inserted BISA cells will be connected to form a number of combinational circuits, called BISA blocks.
- A Logic BIST structure is used to test all BISA blocks.
- If any BISA cell is removed or changed by attackers, a wrong signature will be generated.
- Additionally, BISA cells can also provide decoupling capacitance when original circuits are working.
- Since BISA and original circuits are two independent circuits, BISA's impact is negligible.

BISA Structure and Function

BISA Structure

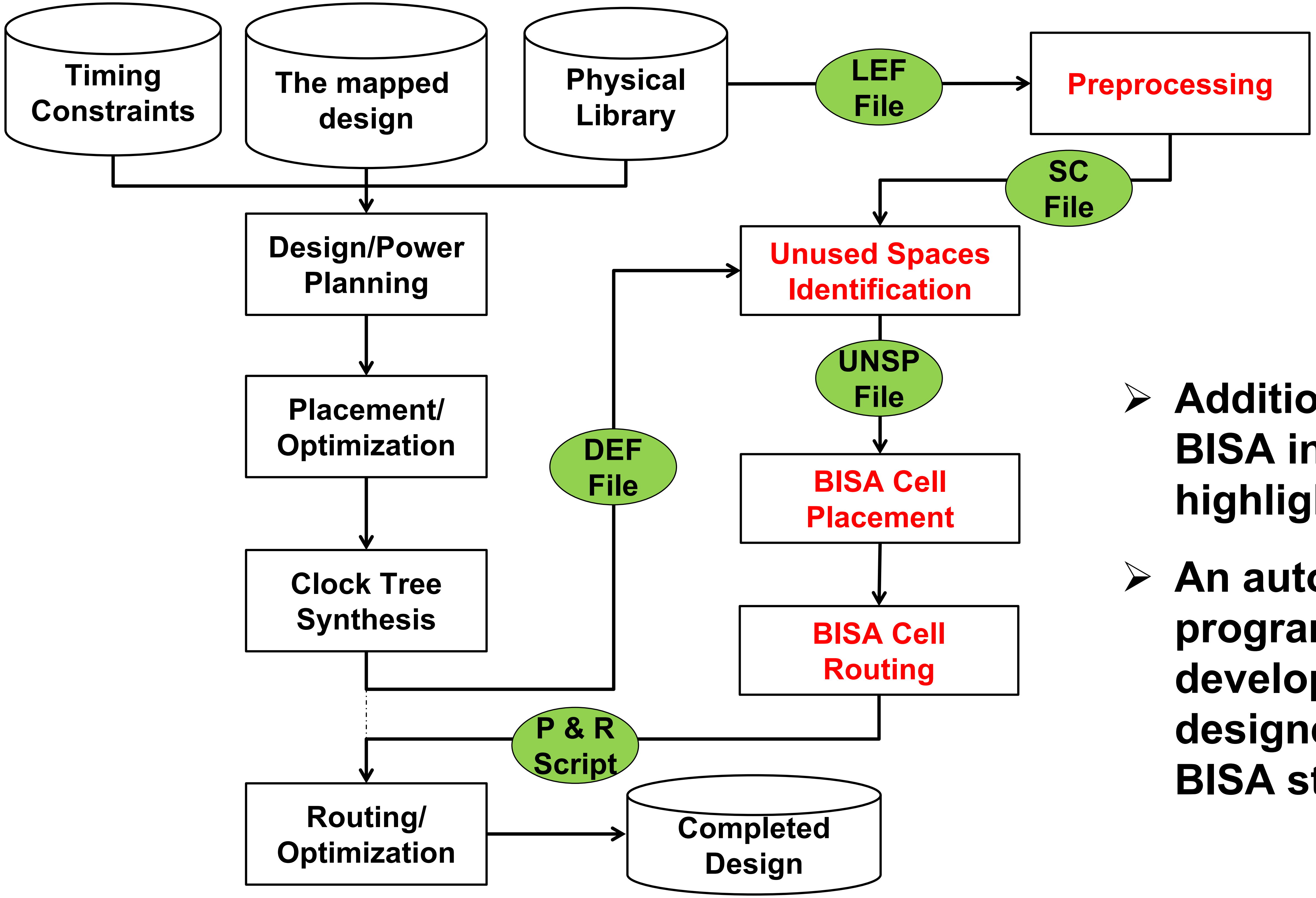


Operation

Mode

	Normal mode	Authentication mode	
		Shift mode	Test mode
Original circuit	Working	Idle	Idle
BISA circuit	Idle	Shift seed/signature	Testing BISA

BISA Design Flow

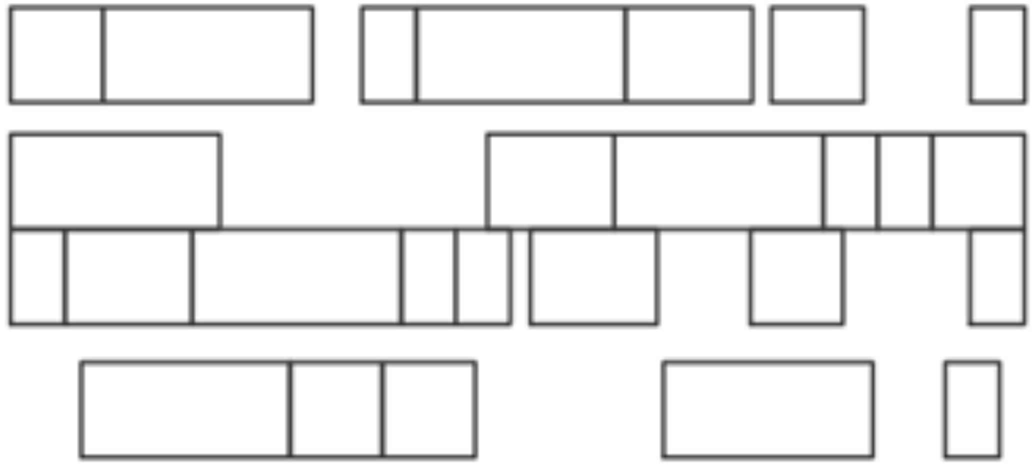


- ➢ Additional steps for BISA insertion are highlighted in red.
- ➢ An automation program has been developed to help designers insert the BISA structure.

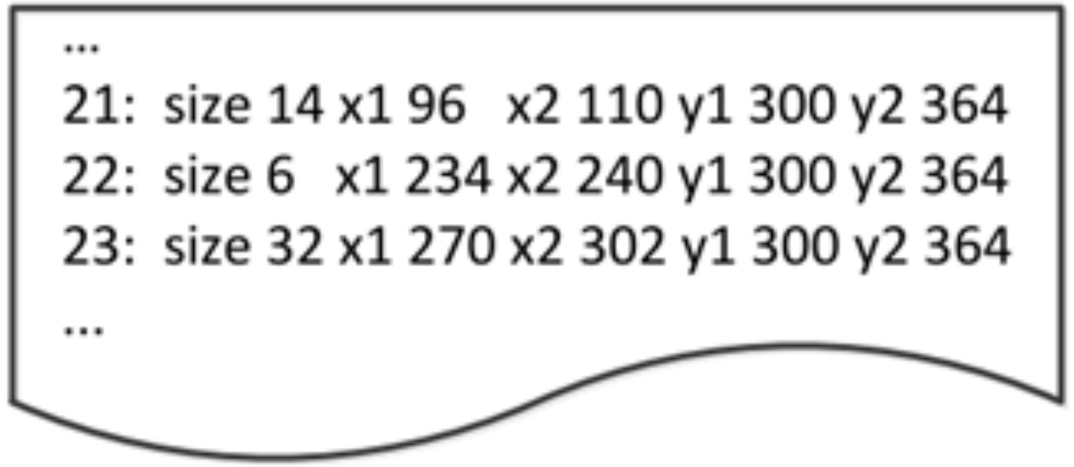
Unused Space Identification

- Input: DEF file
- Output: UNSP file

- After clock tree synthesis, physical design tool writes a DEF file that contains coordinates of all placed standard cells.
- The flow starts to search for and locate all unused spaces of the layout.



(a) Original placement

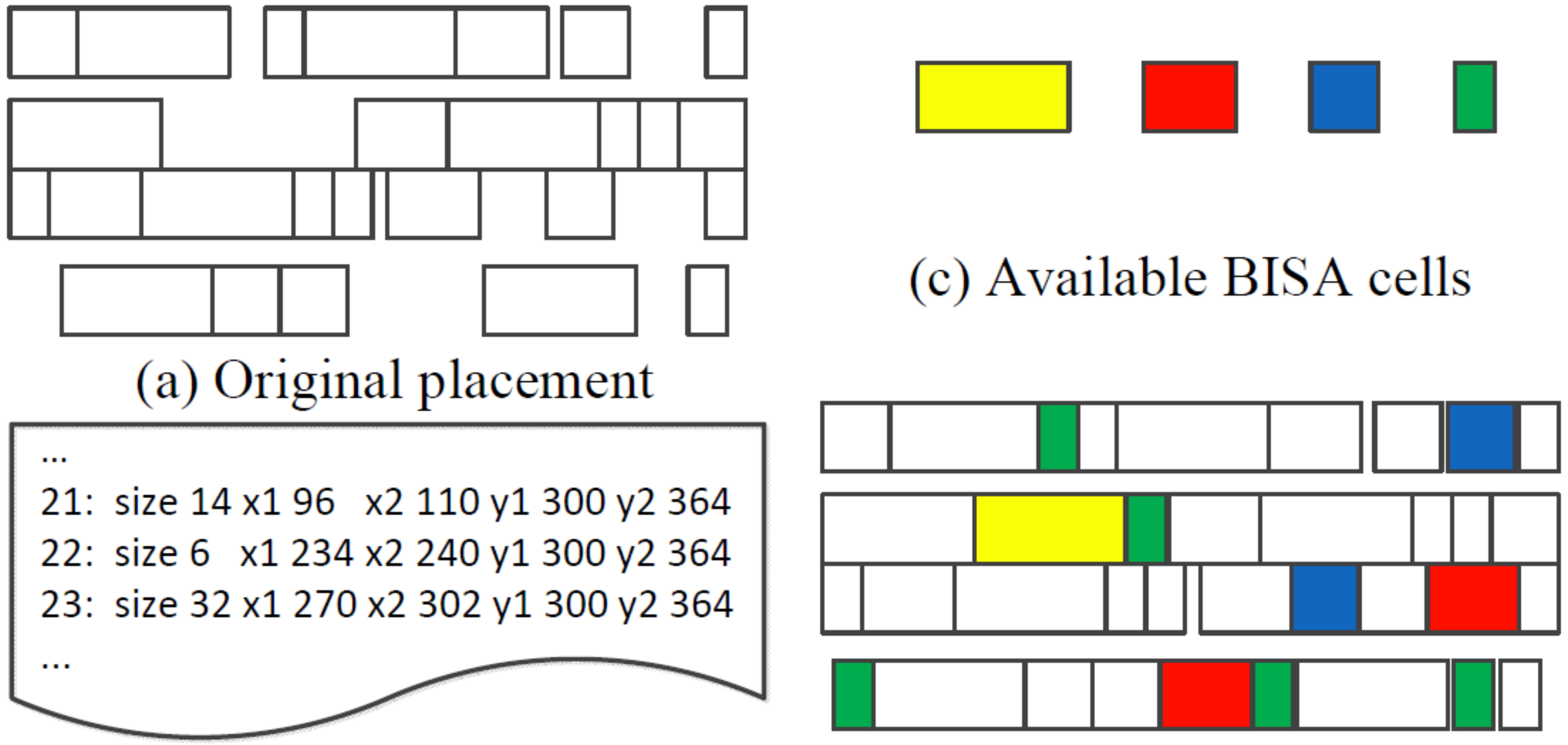


```
...
21:  size 14 x1 96   x2 110 y1 300 y2 364
22:  size 6   x1 234 x2 240 y1 300 y2 364
23:  size 32 x1 270 x2 302 y1 300 y2 364
...
```

(b) An example of unused spaces file (.unsp)

BISA Placement

- **Input:** UNSP file, Output: placement script
- **Tasks**:
  - Insert BISA cells to fill unused spaces as much as possible
  - A dynamic programming algorithm is employed to find an optimal filling solution.



(a) Original placement

```
…
21:  size 14 x1 96   x2 110 y1 300 y2 364
22:  size 6   x1 234 x2 240 y1 300 y2 364
23:  size 32 x1 270 x2 302 y1 300 y2 364
…
```

(b) An example of unused spaces file (.unsp)

(c) Available BISA cells

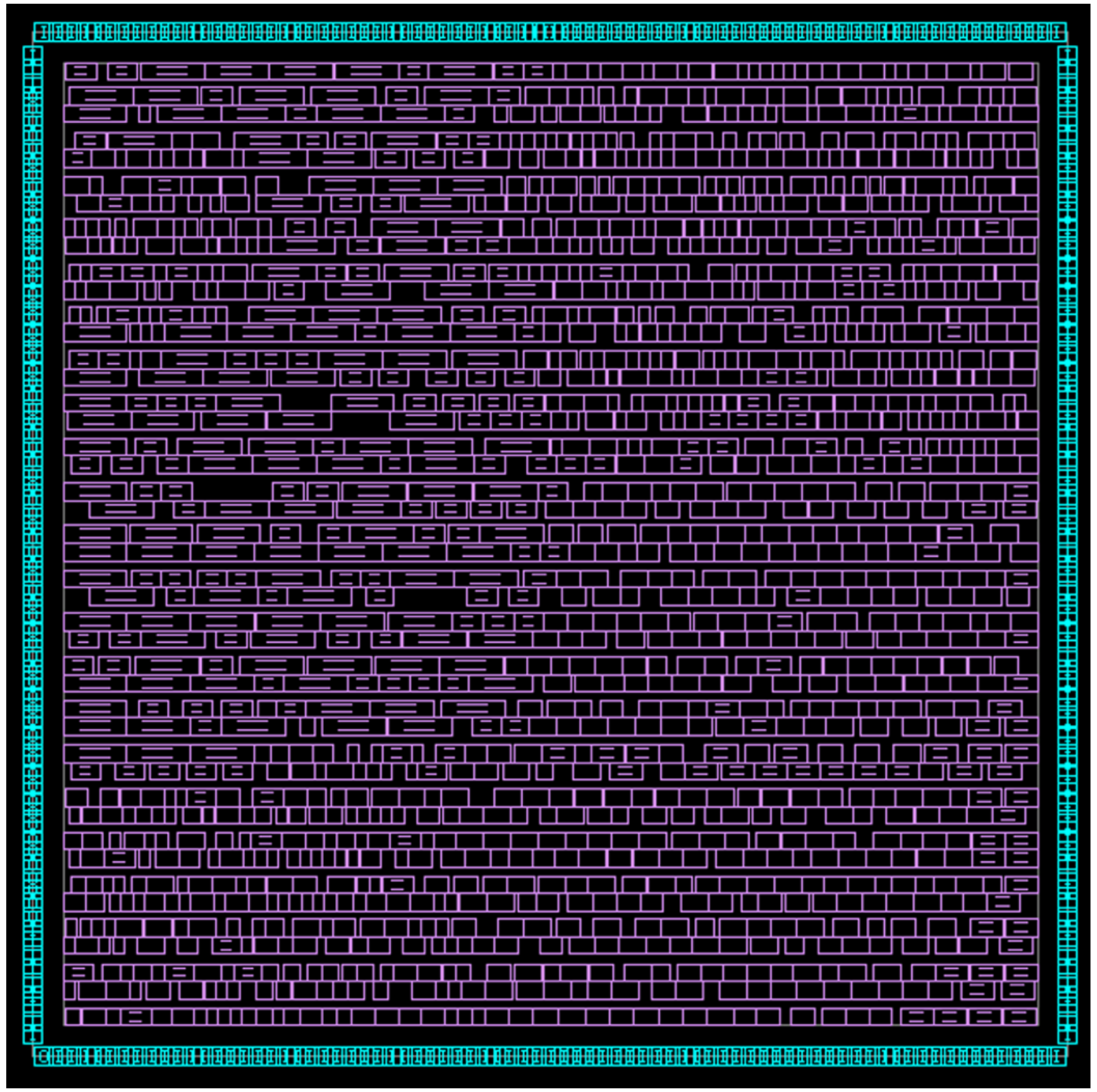
(d) Placement after BISA cells insertion

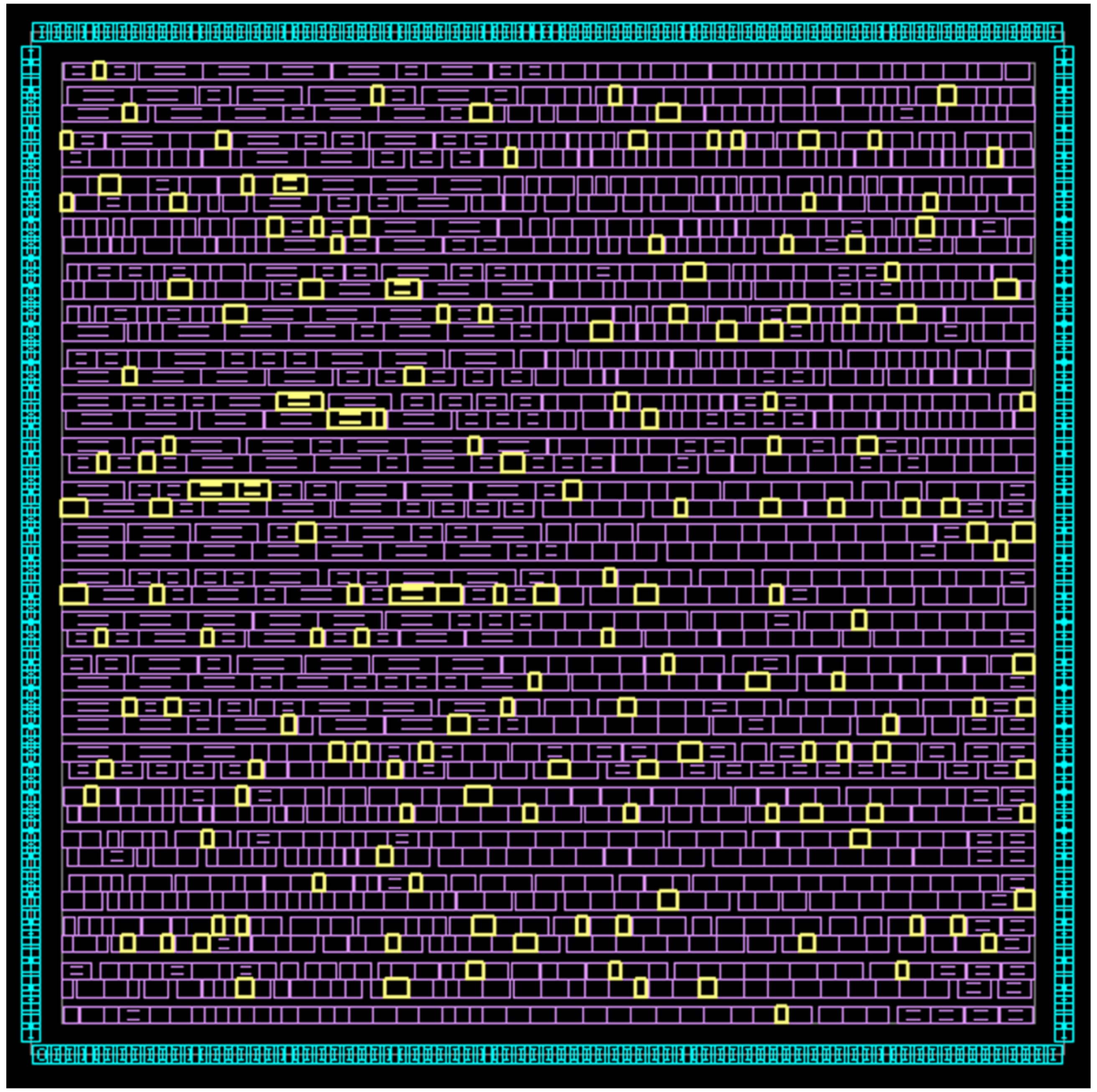
Potential Attacks

- It is difficult for an adversay to identify BISA cells.
  - BISA cells are the same as other circuit cells.
- Assume attackers can identify them:
  - **Removal attack**: Simply removing cells
    - Original circuit: it will change the functinality.
    - BISA circuit: it will change the functinality.
  - **Redesign attack:** changing cells
    - Original circuit: it may change the functinality or chip dimensions.
    - BISA circuit: it may change the functinality.
  - **Resizing attack**: sizing to smaller cells
    - Original circuit: it may impact chip performance.
    - BISA circuit: BISA cells are already minimimum-sized.
  - **TPG/ORA attack:**
    - Any change will lead to a different signature.

Results and Analysis

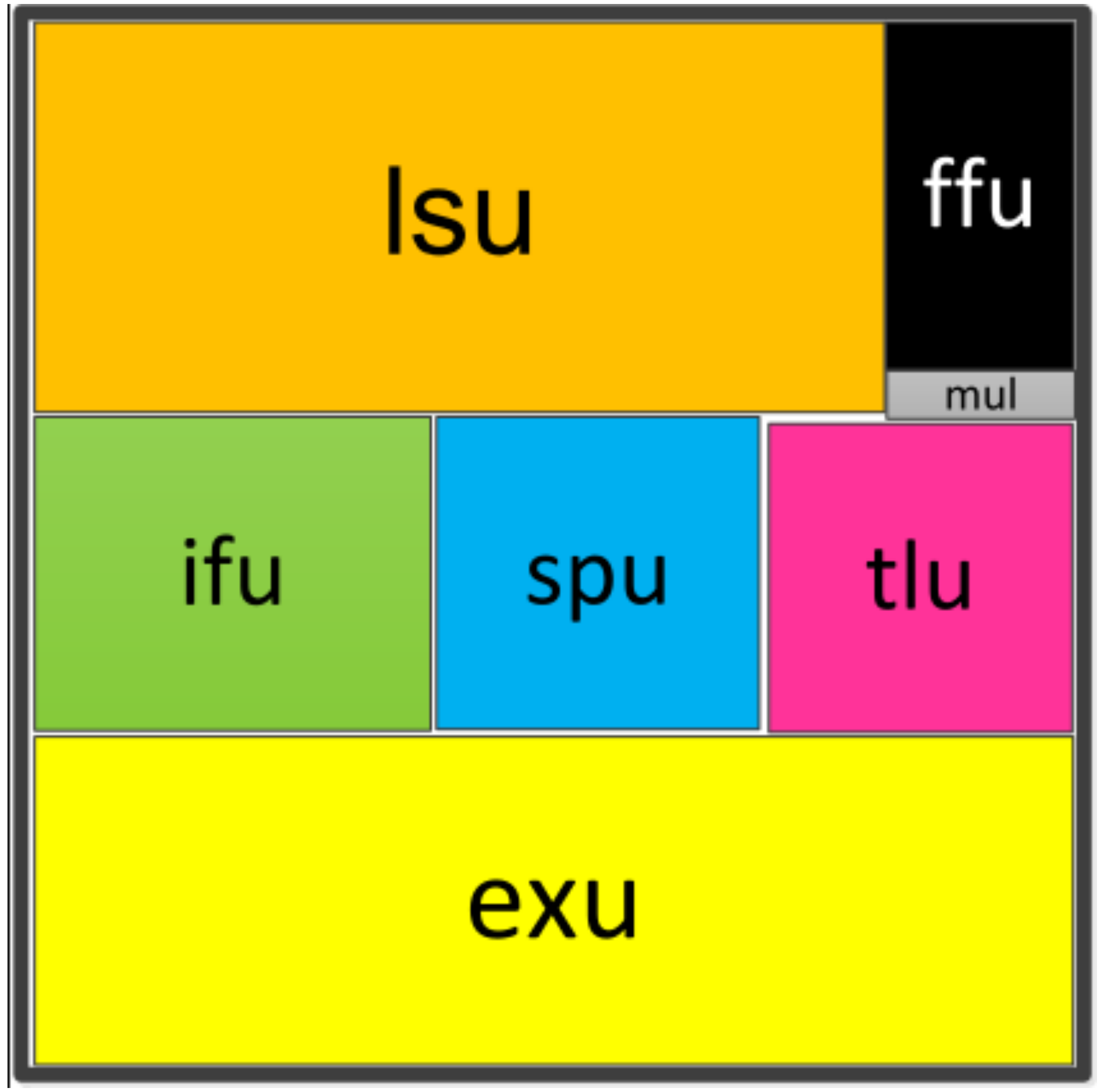
Implementation: DES3_area (from OpenSparc)

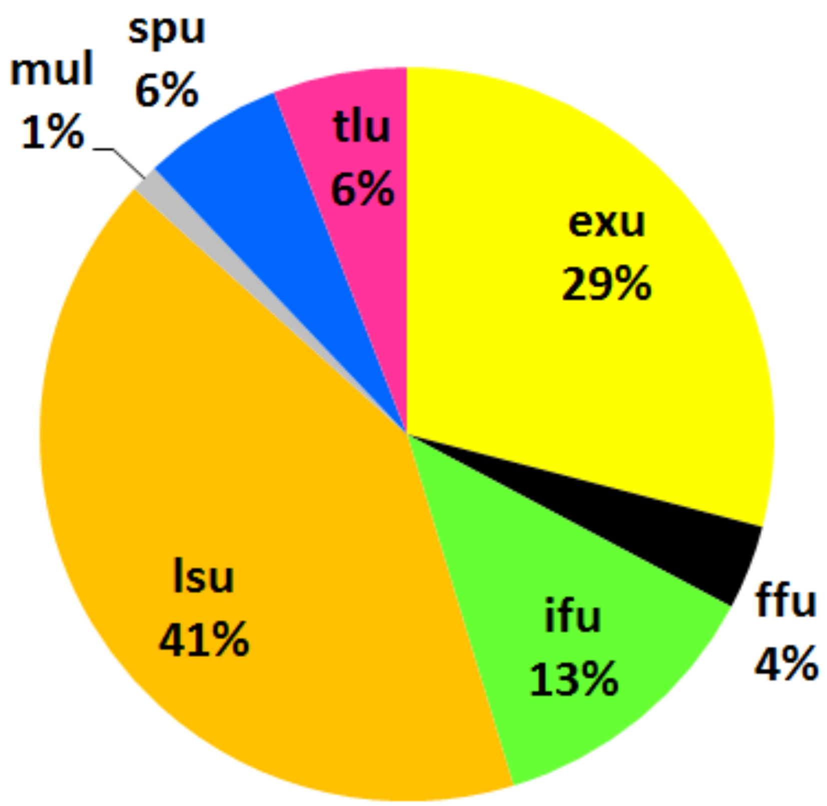




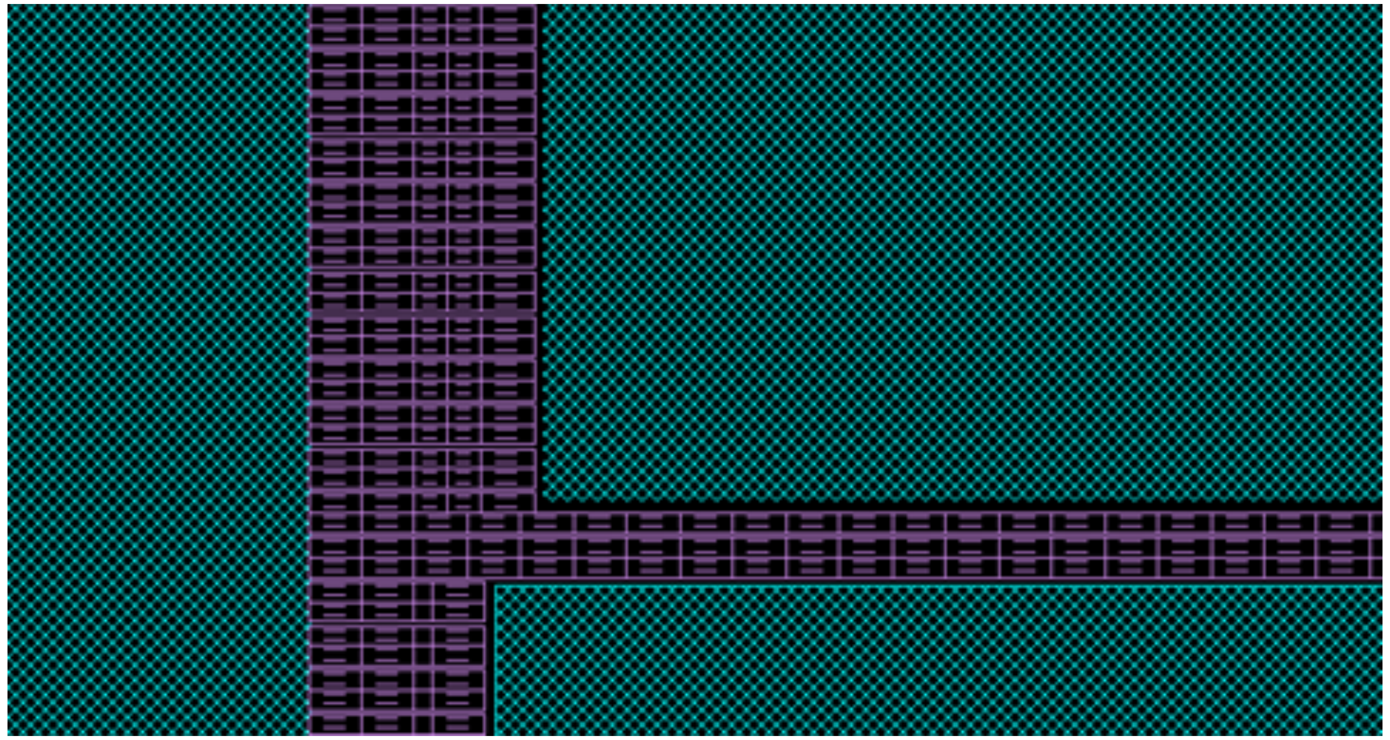
Results and Analysis

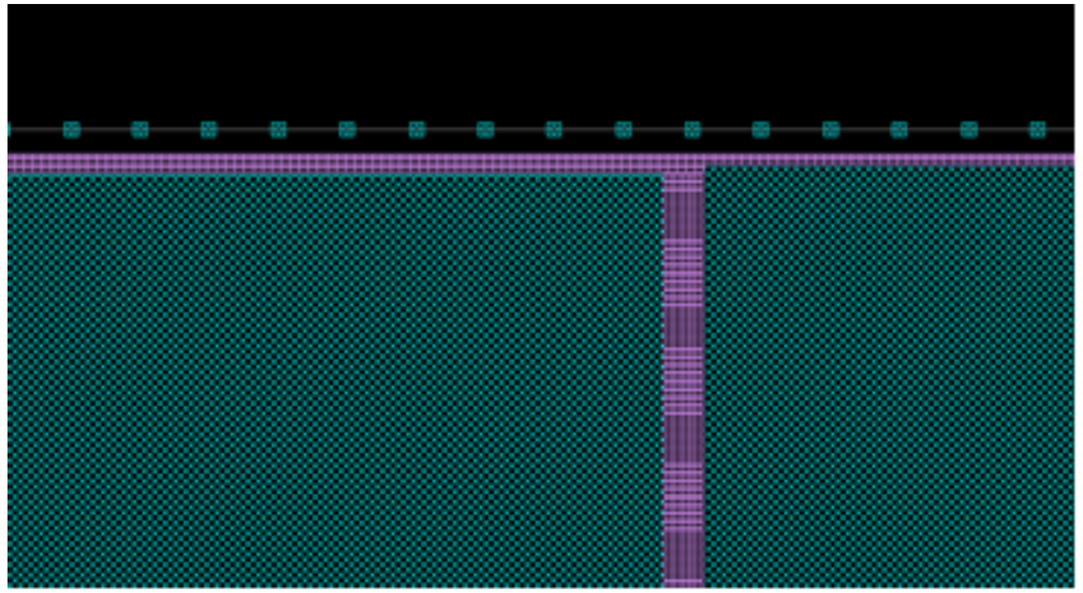
- OpenSparc T1 benchmark:
  - The first 64-bit open-sourced microprocessors released by Oracle
- OpenSparc Core (781,321 cells):
  - 7 sub-modules: lsu, ffu, mul, tlu, spu, ifu, exu
  - Floorplaning:

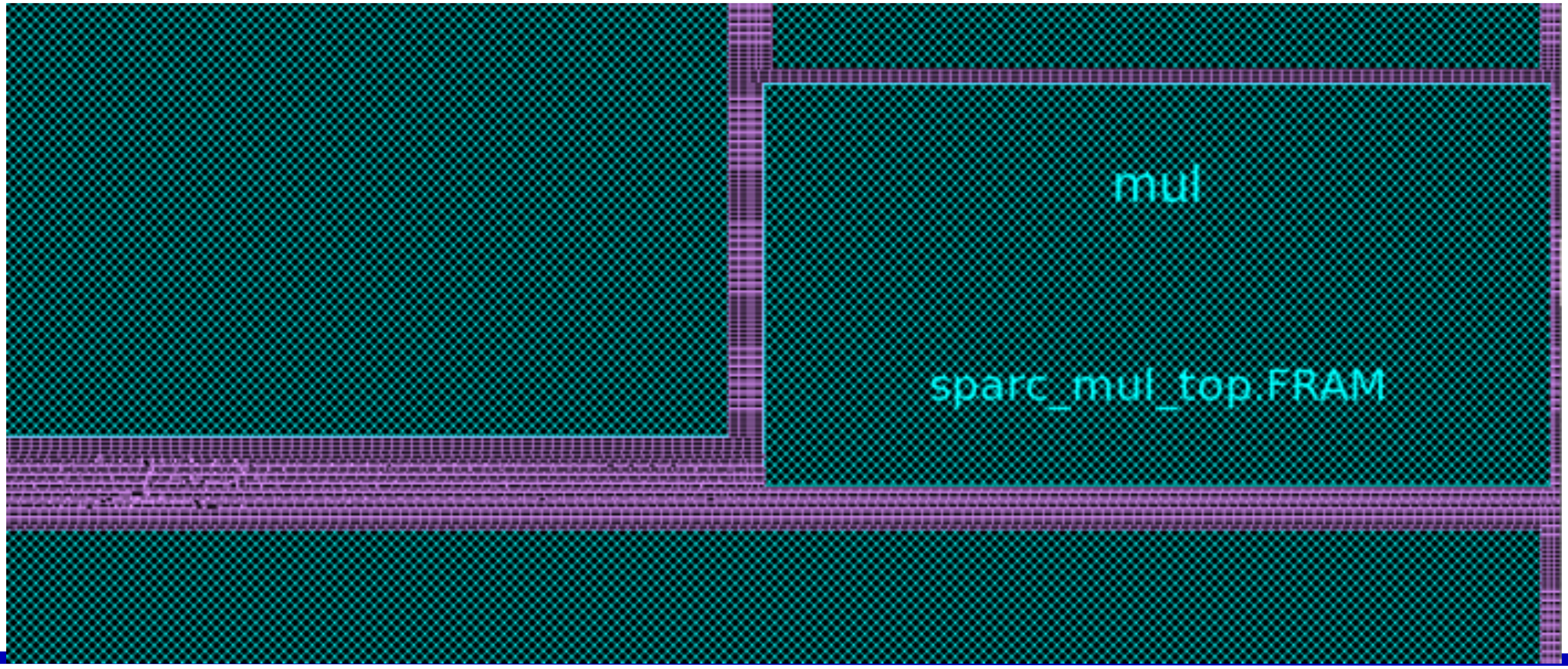




Results and Analysis

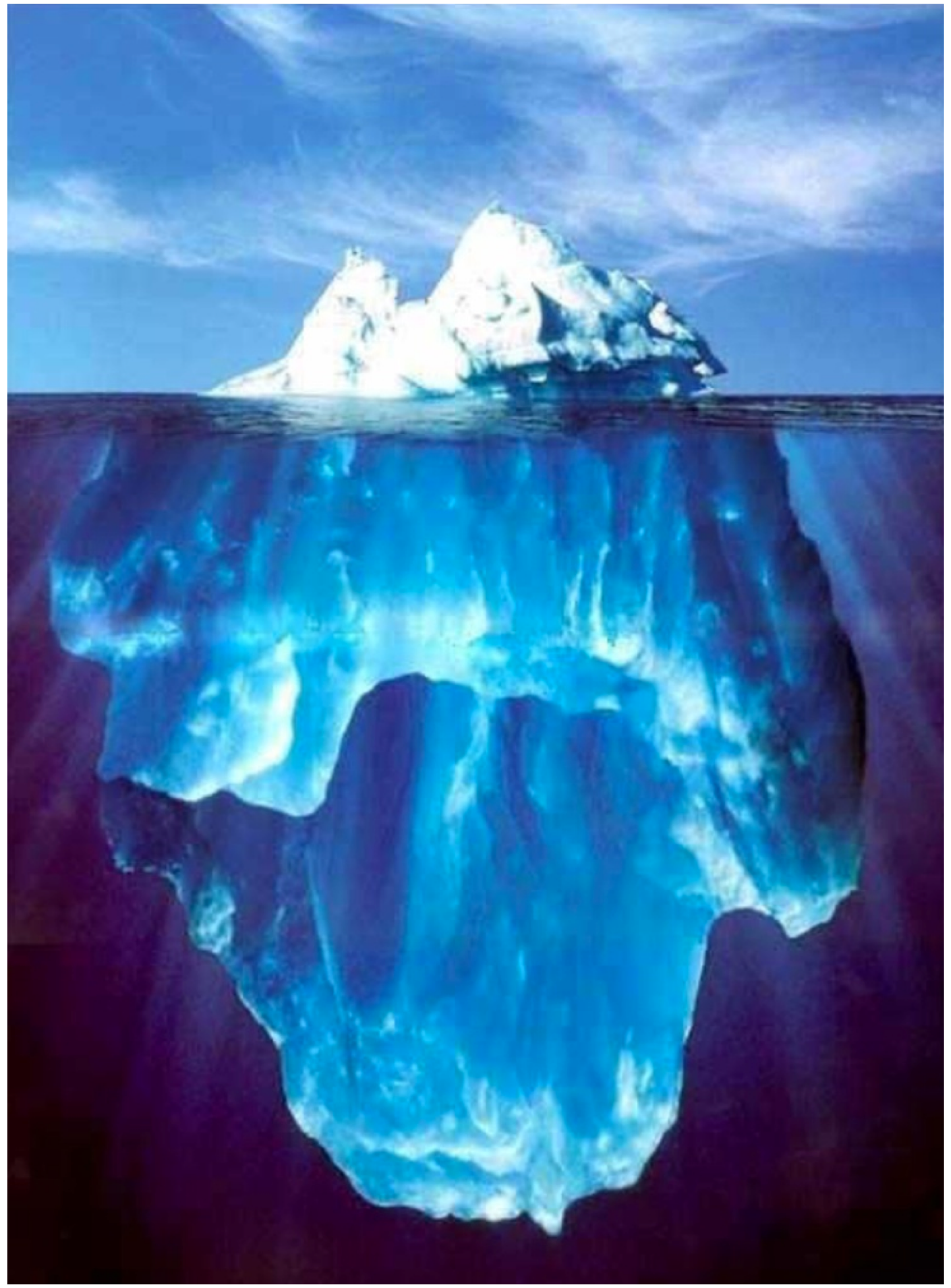






Outline

- Problem Statement and the Fundamentals
- Example Attacks
- Supply Chain Vulnerabilities
- Counterfeit Electronics
- Hardware Trojans
- PUF + ECID
- Logic Obfuscation / IP Encryption
- Research Challenges



- Attack-resilient logic obfuscation
- Reliable PUF
- Better ECID
- Low-cost counterfeit detection approaches
  - New techniques for analog ICs
  - Low cost track and trace
- Detection of hardware Trojans in commercial off the shelf components (COTS)
- Third party IP (3PIP) trust analysis

References

- P. Mishra, S. Bhunia, and M. Tehranipoor, Hardware IP Security and Trust: Validation and Test, Springer, 2017.
- D. Forte, S. Bhunia, and M. Tehranipoor, Hardware Protection through Obfuscation, Springer, 2017.
- M. Tehranipoor, U. Guin, and D. Forte, Counterfeit Integrated Circuits: Detection and Avoidance, Springer, Dec. 2014
- M. Tehranipoor, H. Salmani, and X. Zhang, IC Authentication: Hardware Trojan and Counterfeit Detection, Springer, Jan. 2014.
- M. Tehranipoor and C. Wang, Introduction to Hardware Security and Trust, Springer, June 2011.
- M. Tehranipoor, U. Guin, and S. Bhunia, "Invasion of the Hardware Snatchers: Fake Hardware Could Open the Door to Malicious Malware and Critical Failure," IEEE Spectrum, 2017.
- B. Shakya, H. Salmani, D. Forte, S. Bhunia, and M. Tehranipoor, "Benchmarking of Hardware Trojans and Maliciously Affected Circuits," Journal of Hardware and Systems Security (HaSS), 2017.
- Z. Guo, J. Di, M. Tehranipoor, and D. Forte, "Obfuscation-based Protection Framework Against Printed Circuit Boards Unauthorized Operation and Reverse Engineering," ACM Transactions on Design Automation of Electronic Systems (TODAES), 2017.
- K. Yang, D. Forte, and M. Tehranipoor, "CDTA: A Comprehensive Solution for Counterfeit Detection, Traceability and Authentication in IoT Supply Chain," ACM Transactions on Design Automation of Electronic Systems (TODAES), 2017.
- U. Guin, S. Bhunia, D. Forte, and M. Tehranipoor, "SMA: A System-Level Mutual Authentication for Protecting Electronic Hardware and Firmware," Transactions on Dependable and Secure Computing (TDSC), Oct. 2016.
- M. Alam, H. Shen, N. Asadi, M. Tehranipoor, and D. Forte, "Impact of X-ray Tomography on the Reliability of Integrated Circuits," IEEE Transaction on Device and Materials Reliability, vol. 7, Issue 1, March 2017.
- N. Asadi, M. Tehranipoor, and D. Forte, "PCB Reverse Engineering Using Non-destructive X-ray Tomography and Advanced Image Processing," IEEE Transactions on Components, Packaging and Manufacturing Technology (TCPMT), Vol. 7, Issue 2, Feb. 2017.
- K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor, "Hardware Trojans: Lessons Learned After One Decade of Research," ACM Transactions on Design Automation of Electronic Systems (TODAES), Vol. 22, Issue 1, Dec. 2016.

References

- Y. Xie, C. Bao, C. Serafy, T. Lu, A. Srivastava, and M. Tehranipoor, “Security and Vulnerability Implications of 3D ICs,” IEEE Trans. on Multi-Scale Computing Systems (TMSCS), Vol. 2, Issue 2, June 2016.
- U. Guin, Q. Shi, D. Forte, and M. Tehranipoor, “FORTIS: A Comprehensive Solution for Establishing Forward Trust for Protecting IPs and ICs,” ACM Transactions on Design Automation of Electronic Systems (TODAES), May 2016.
- H. Salmani and M. Tehranipoor, “Vulnerability Analysis of a Circuit Layout to Hardware Trojan Insertion,” IEEE Transactions on Information Forensics & Security (TIFS), Vol. 11, Issue 6, June 2016.
- T. Rahman, F. Rahman, D. Forte, and M. Tehranipoor, “An Aging-Resistant RO-PUF for Reliable Key Generation,” IEEE Transactions on Emerging Topics in Computing (TETC), Vol. 4, Issue 3, July 2016.
- U. Guin, D. Forte, and M. Tehranipoor, “Design of Accurate Low-Cost On-Chip Structures for Protecting Integrated Circuits Against Recycling,” IEEE Transactions on VLSI (TVLSI), Vol. 24, Issue 4, April 2016.
- S. Quadir, J. Chen, D. Forte, N. Asadi, S. Shahbaz, L. Wang, J. Chandy, and M. Tehranipoor, “A Survey on Chip to System Reverse Engineering,” ACM Journal on Emerging Technologies in Computing Systems (JETC), Vol 13, Issue 1, Dec. 2016.
- K. Xiao, D. Forte, and M. Tehranipoor, “A Novel Built-In Self-Authentication Technique to Prevent Inserting Hardware Trojans,” IEEE Transactions on CAD (TCAD), vol. 33, no. 12, pp. 1178-1791, 2014.
- U. Guin, K. Huang, D. DiMase, J. Carulli, M. Tehranipoor, Y. Makris, “Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain,” Proceedings of IEEE, vol. 102, no. 8, pp. 1207-1228, 2014.
- Z. Collier, D. DiMase, S. Walters, M. Tehranipoor, J. Lambert, and I. Linkov, “Risk-Based Cybersecurity Standards: Policy Challenges and Opportunities,” IEEE Computer Magazine, pp. 70-76, Jan. 2014.
- U. Guin, D. DiMase, and M. Tehranipoor, “Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead,” Journal of Electronic Testing: Theory and Applications (JETTA), vol. 30, no. 1, pp. 9-23, Feb. 2014.
- U. Guin, D. DiMase, and M. Tehranipoor, “A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment,” Journal of Electronic Testing: Theory and Applications (JETTA), vol. 30, no. 1, pp. 25-40, Jan. 2014. U. Guin, D. DiMase, and M. Tehranipoor, “A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment,” Journal of Electronic Testing: Theory and Applications (JETTA), vol. 30, no. 1, pp. 25-40, Jan. 2014

References

- Francis Wolff, Christos Papachristou, Rajat Subhra Chakraborty, and Swarup Bhunia, “Towards Trojan-Free Trusted ICs: Problem Analysis and a Low-Overhead Detection Scheme”, Design Automation and Test in Europe (DATE), pp. 1362-1365, 2008.
- Rajat Subhra Chakraborty, Somnath Paul, and Swarup Bhunia, “On-Demand Transparency for Improving Hardware Trojan Detectability”, IEEE Hardware Oriented Security and Trust (HOST) Workshop, pp. 48-50, 2008.
- Rajat Subhra Chakraborty, Francis Wolff, Somnath Paul, Christos Papachristou and Swarup Bhunia, "MERO: A Statistical Approach for Hardware Trojan Detection", Workshop on Cryptographic Hardware and Embedded Systems (CHES), 2009.
- Rajat Subhra Chakraborty and Swarup Bhunia, "Security against Hardware Trojan through a Novel Application of Design Obfuscation," IEEE International Conference on Computer Aided Design (ICCAD), pp. 113-116, 2009.
- Seetharam Narasimhan, Dongdong Du, Rajat Subhra Chakraborty, Somnath Paul, Francis Wolff, Chris Papachristou, Kaushik Roy and Swarup Bhunia, “Multiple-Parameter Side-Channel Analysis: A Non-invasive Hardware Trojan Detection Approach”, IEEE Symposium on Hardware Oriented Security and Trust (HOST), 2010.
- Dongdong Du, Seetharam Narasimhan, Rajat Subhra Chakraborty and Swarup Bhunia, “Self-Referencing: A Scalable Side-Channel Approach for Hardware Trojan Detection”, Workshop on Cryptographic Hardware and Embedded Systems (CHES), 2010.
- Seetharam Narasimhan, Xinmu Wang, Dongdong Du, Rajat Subhra Chakraborty, and Swarup Bhunia, “TeSR: A Robust Temporal Self-Referencing Approach for Hardware Trojan Detection”, 4th IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2011.
- M. Tehranipoor, H. Salmani, X. Zhang, X. Wang, R. Karri, J. Rajendran and K. Rosenfeld, "Trustworthy Hardware: Trojan Detection Solutions and Design-for-Trust Challenges", IEEE Computer Magazine , Vol. 44, Issue 7, pp. 66-74, 2011.
- R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor" Trustworthy Hardware: Identifying and Classifying Hardware Trojans", IEEE Computer Magazine, Vol. 43, Issue 10, pp. 39-46, October 2010.

?

Mark M. Tehranipoor, PhD
Intel Charles E. Young Preeminence Endowed Chair Professor in Cybersecurity
Electrical and Computer Engineering Department, University of Florida
Florida Institute for Cybersecurity (FICS) Research
Phone: 352-392-2585
FICS Research: http://fics-institute.org/
Personal Page: http://tehranipoor.ece.ufl.edu/index.html