Hardware Root-of-Trust for Cyber Security

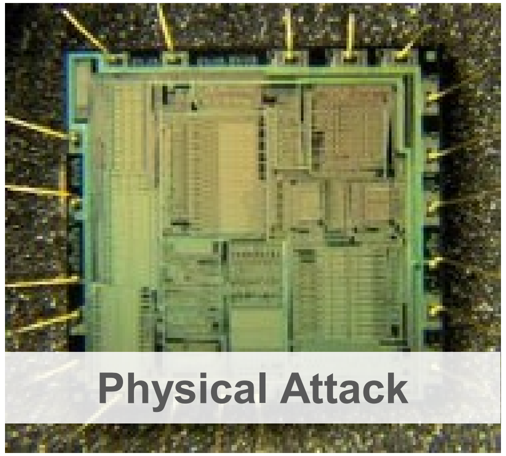
Mark M. Tehranipoor
Intel Charles E. Young Endowed Chair Professor in Cybersecurity
Director, Florida Institute for Cybersecurity Research
Electrical and Computer Engineering Department

Example Hardware Attacks

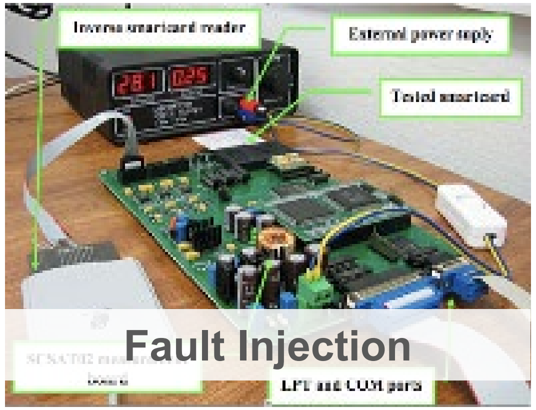
Trojans

Untrusted Foundry

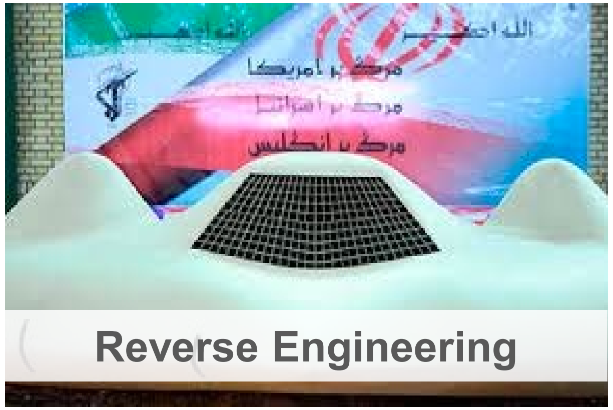
Counterfeit ICs

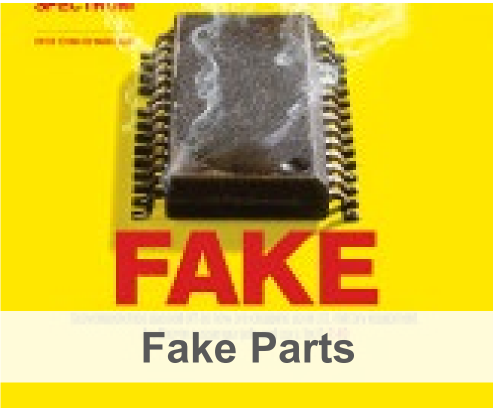

Physical Attack

Side-channel



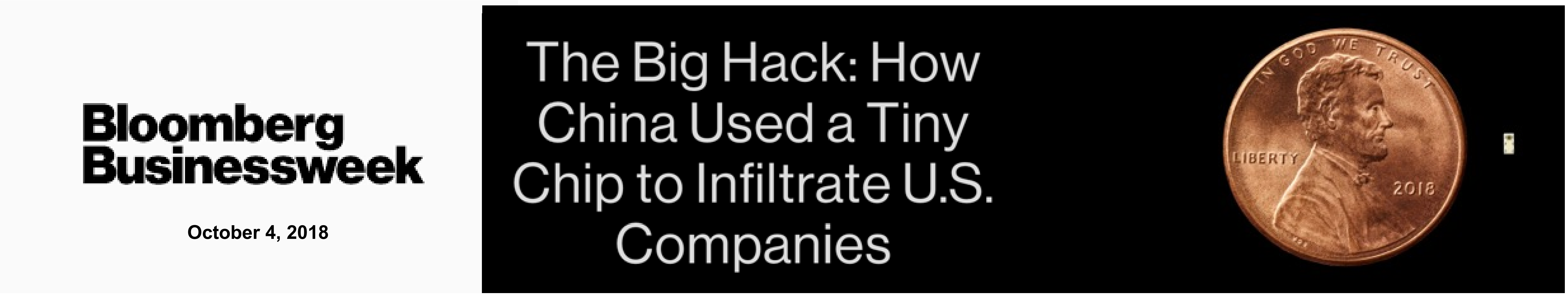
Fault Injection


Reverse Engineering



Fake Parts

The Big Hack

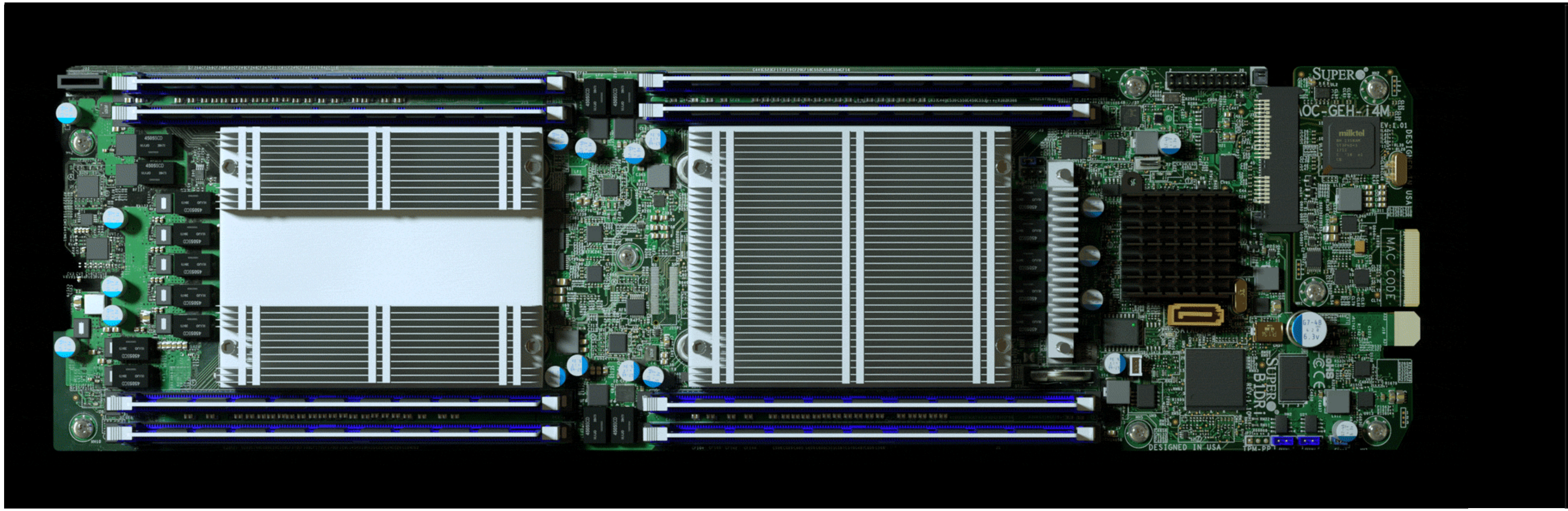


Bloomberg Businessweek

October 4, 2018

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

IN GOD WE TRUST
LIBERTY
2018

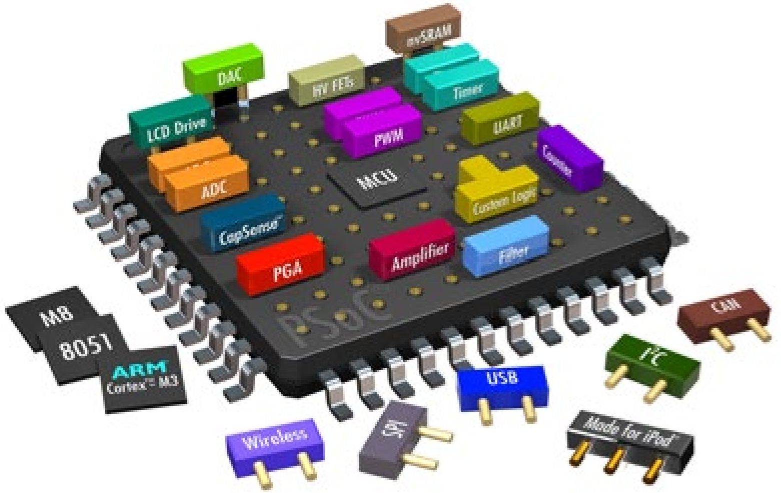


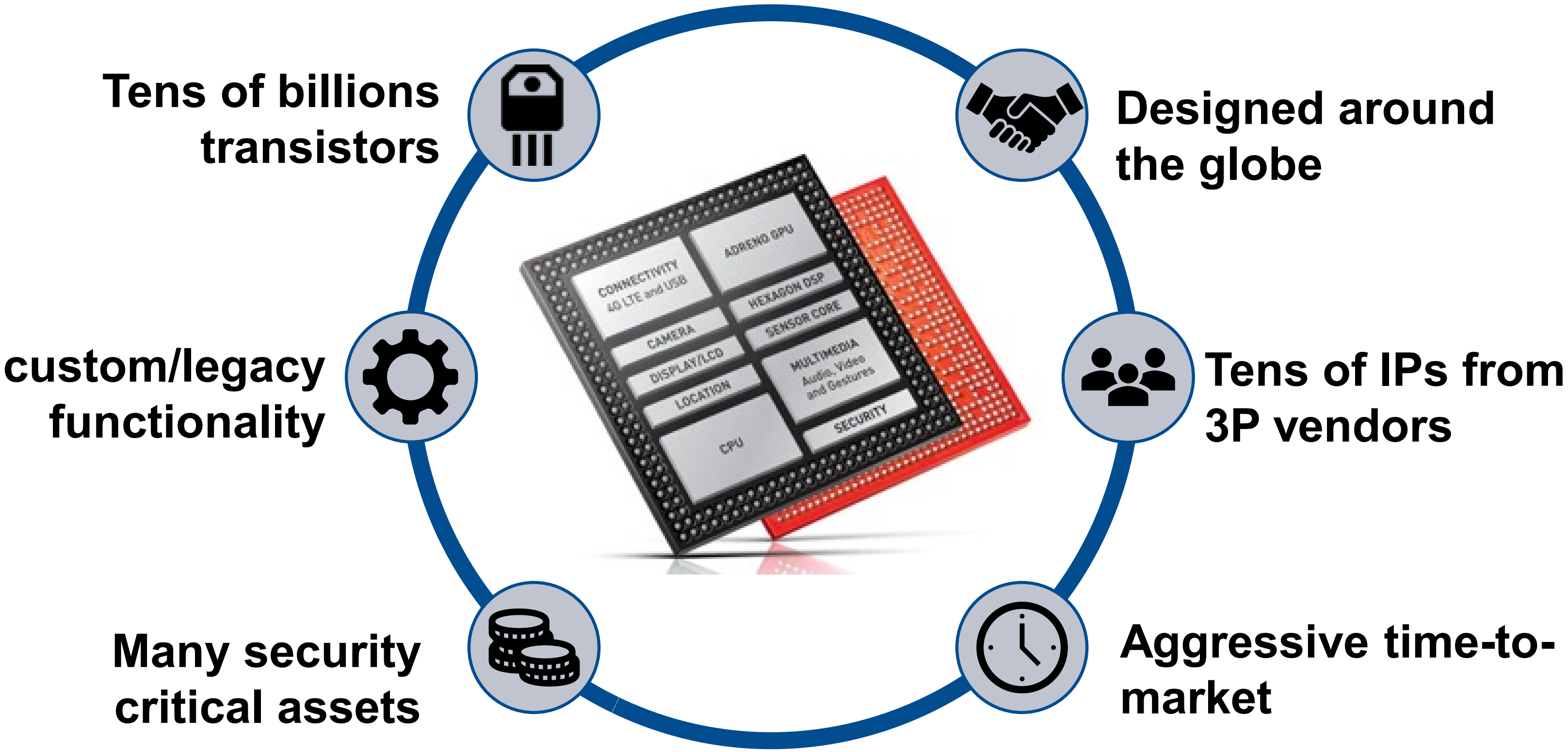
Bloomberg Businessweek

The Big Hack

How China used a tiny chip to infiltrate America's top companies

SoC Security is a Challenge





Tens of billions transistors

Designed around the globe

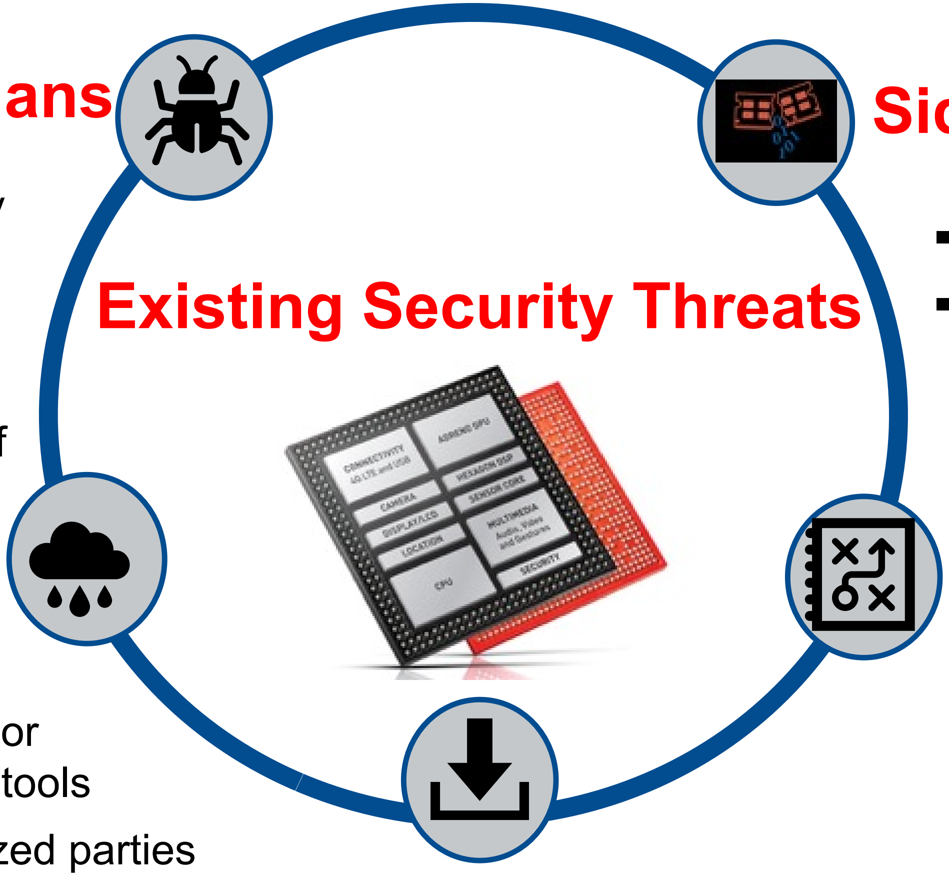
custom/legacy functionality

Tens of IPs from 3P vendors

Many security critical assets

Aggressive time-to-market

Possible Attacks



Existing Security Threats

Hardware Trojans

- Malicious modification of design by adversaries
- Inserted by rogue employees of design house or foundry
- Intentionally introduced→ Denial of Service, information leakage

Information Leakage

- Created intentionally by 3PIP vendor or induced unintentionally by CAD tools
- Reveal of information to unauthorized parties

Side Channel

- No modification of design
- Extraction of secret information through communication channels of ICs

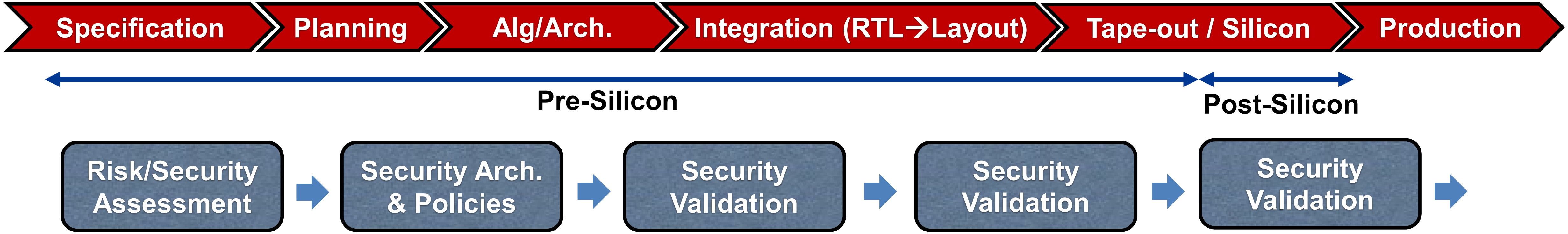
Exploitation of Test/Debug Infrastructure

- Scan, Compression, JTAG etc.
- Exploitation of controllability and observability of a design maliciously

Fault Injection

- Power/Clock glitch, temperature variation, light/leaser/EM injection by malicious intention
- Violation of confidentiality, integrity, and etc.

Security along SoC Design Life-cycle



Specification → Planning → Alg/Arch. → Integration (RTL→Layout) → Tape-out / Silicon → Production

Pre-Silicon

Post-Silicon

Risk/Security Assessment → Security Arch. & Policies → Security Validation → Security Validation → Security Validation →

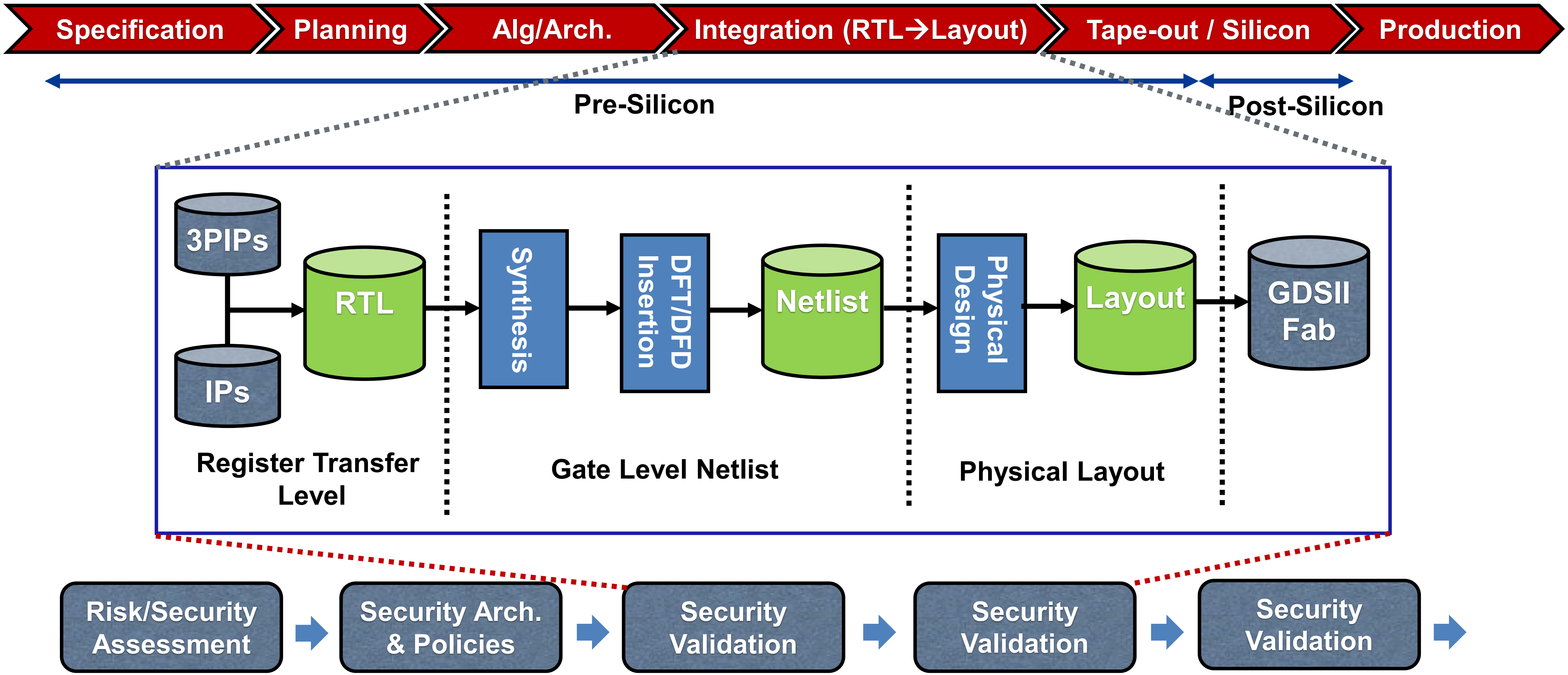
Risk Assessment
Includes definition of assets, threat model, adversaries, and security policies

Secure Architecture
Threat Modeling; Define architecture support for security; Review architecture level security Policies

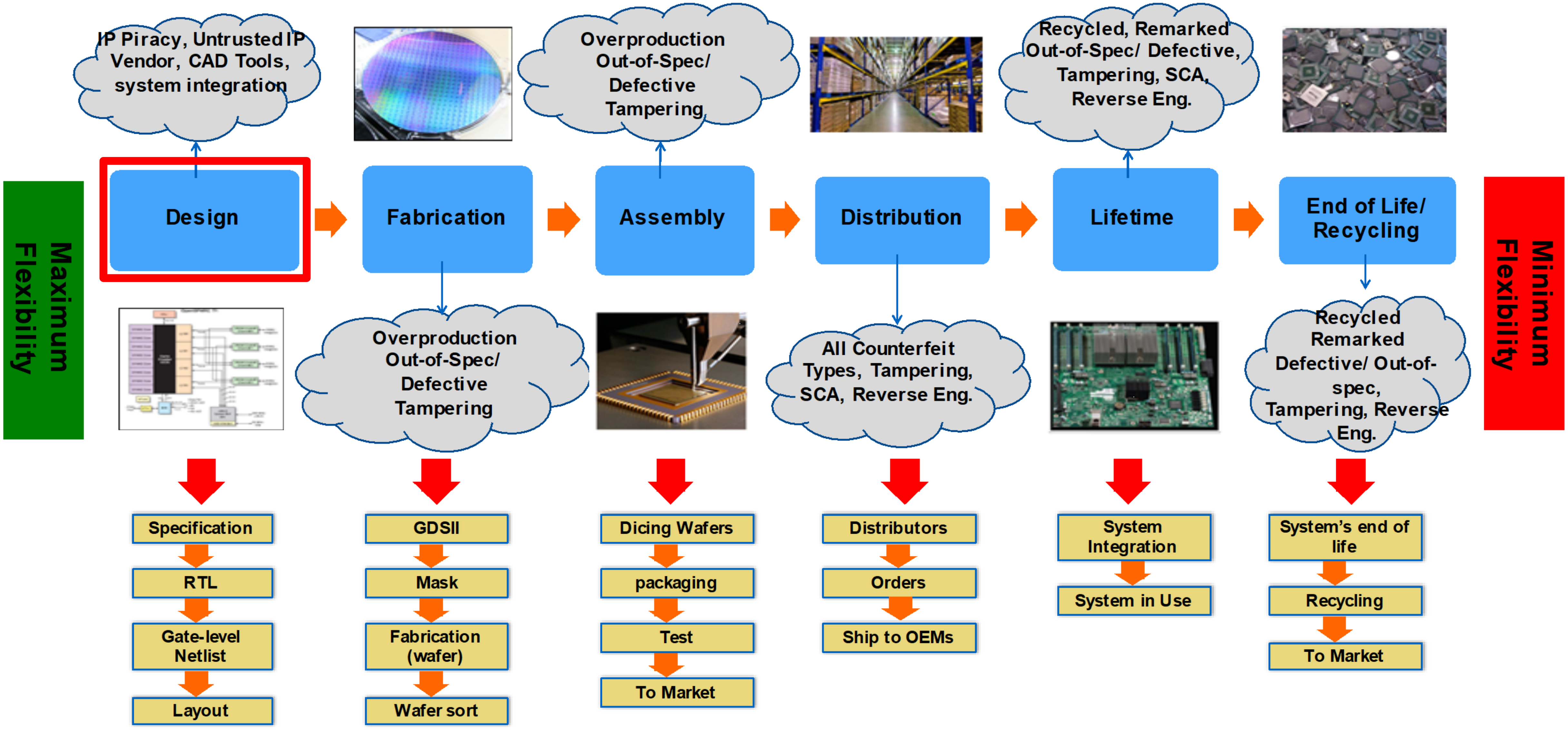
Pre-silicon Security Verification:
Threat Modeling; Design review; Security verification against attacks at different stages of the design process;

Post-Silicon Security Verification:
Fuzzy test, Negative test, and penetration test

Security along SoC Design Life-cycle



Understand Supply Chain Vulnerabilities



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

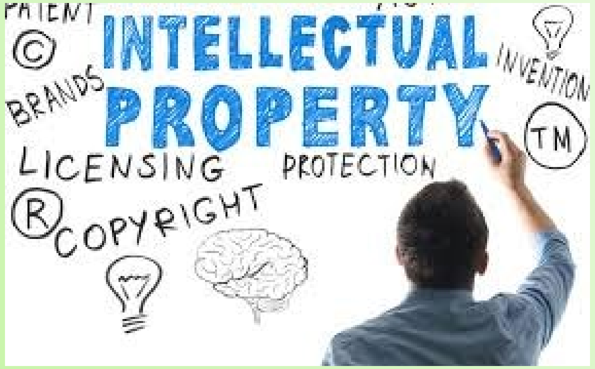
Distribution
All Counterfeit Types, Tampering, SCA, Reverse Eng.
Distributors → Orders → Ship to OEMs

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

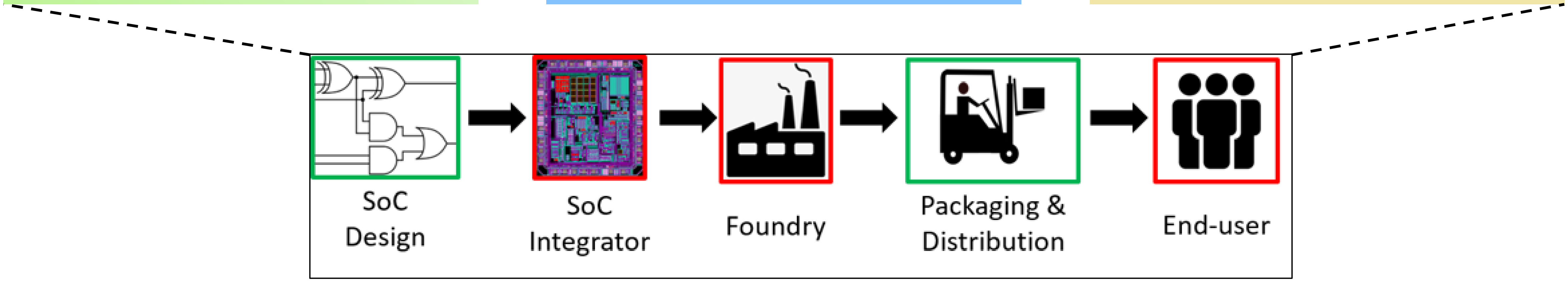
Solutions, with Lifecycle in Mind



Protect the IP

Protect the Assets

Protect the Supply Chain

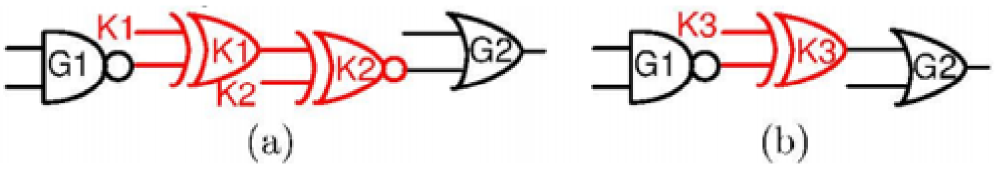


Protect IP

Logic Locking or Obfuscation

❑ Runs of Key gates-

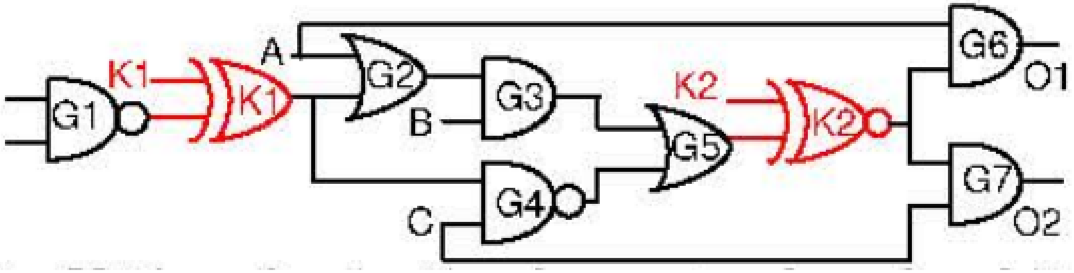
- ❑ keys gates connected back-to-back
- ❑ K1, K2 forms a run that can be replaced by K3



(a) (b)

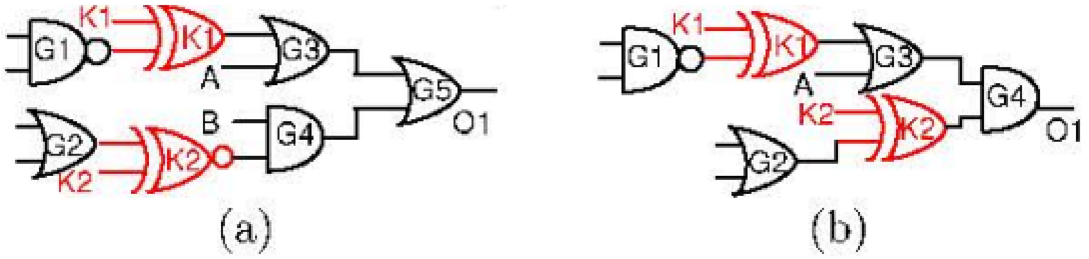
❑ Dominating Key gates-

- ❑ K2 lies on every path from K1 to outputs
- ❑ K2 is dominating key gate whose bit value can only be determined after muting K1



❑ Mutable convergent Key gates-

- ❑ K1 & K2 converges at some other gate, such that K1's bit value can be determined by muting K2 and vice versa

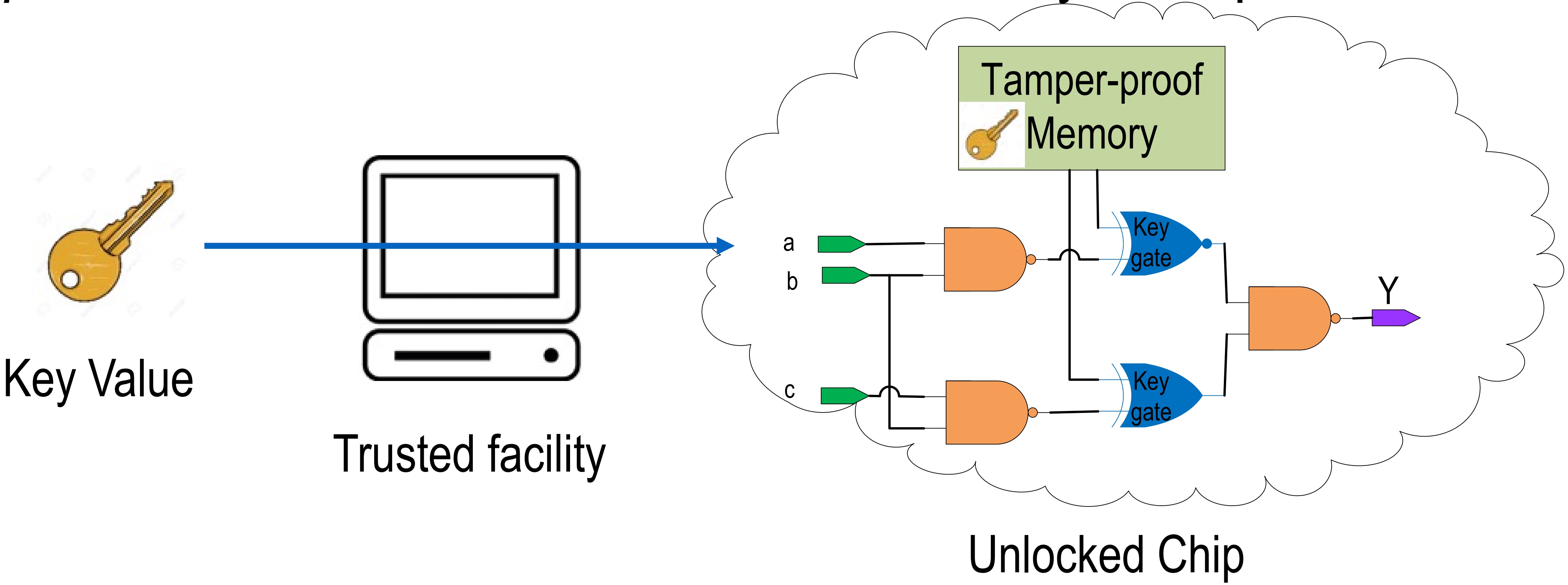


(a) (b)

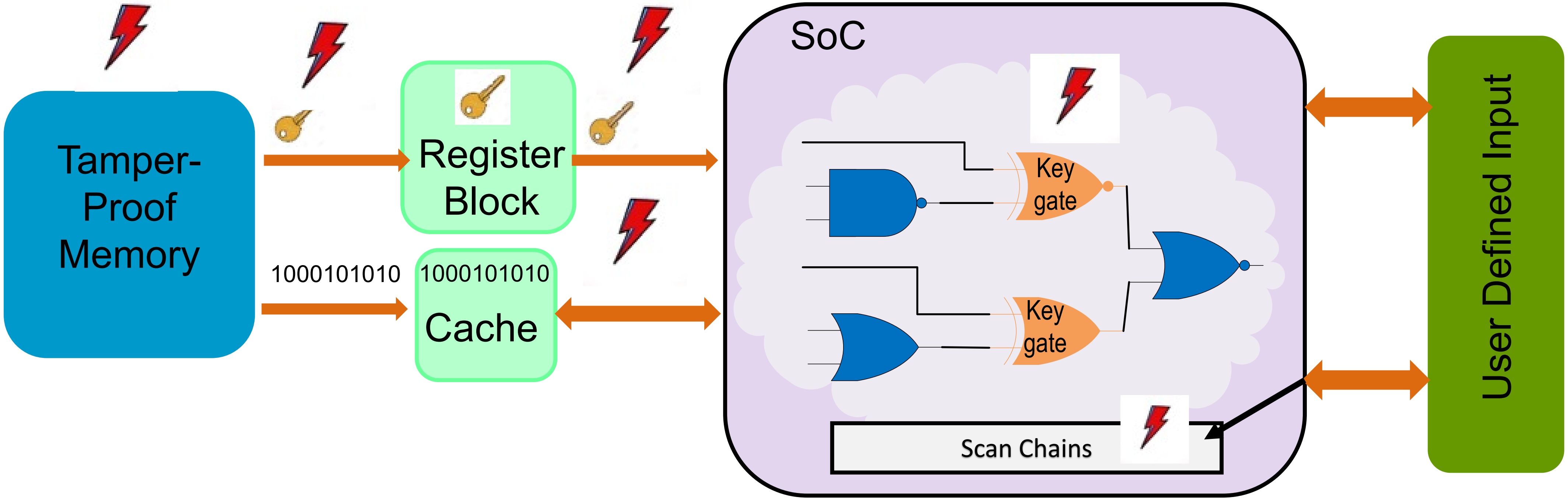
Protect IP, Against Piracy

Logic Locking

- Inserting key gates to lock the design and functionality of the chip
- Writing the correct key in a *tamper-proof non-volatile memory on the chip* after fabrication to unlock the functionality of chip



Potential Threats

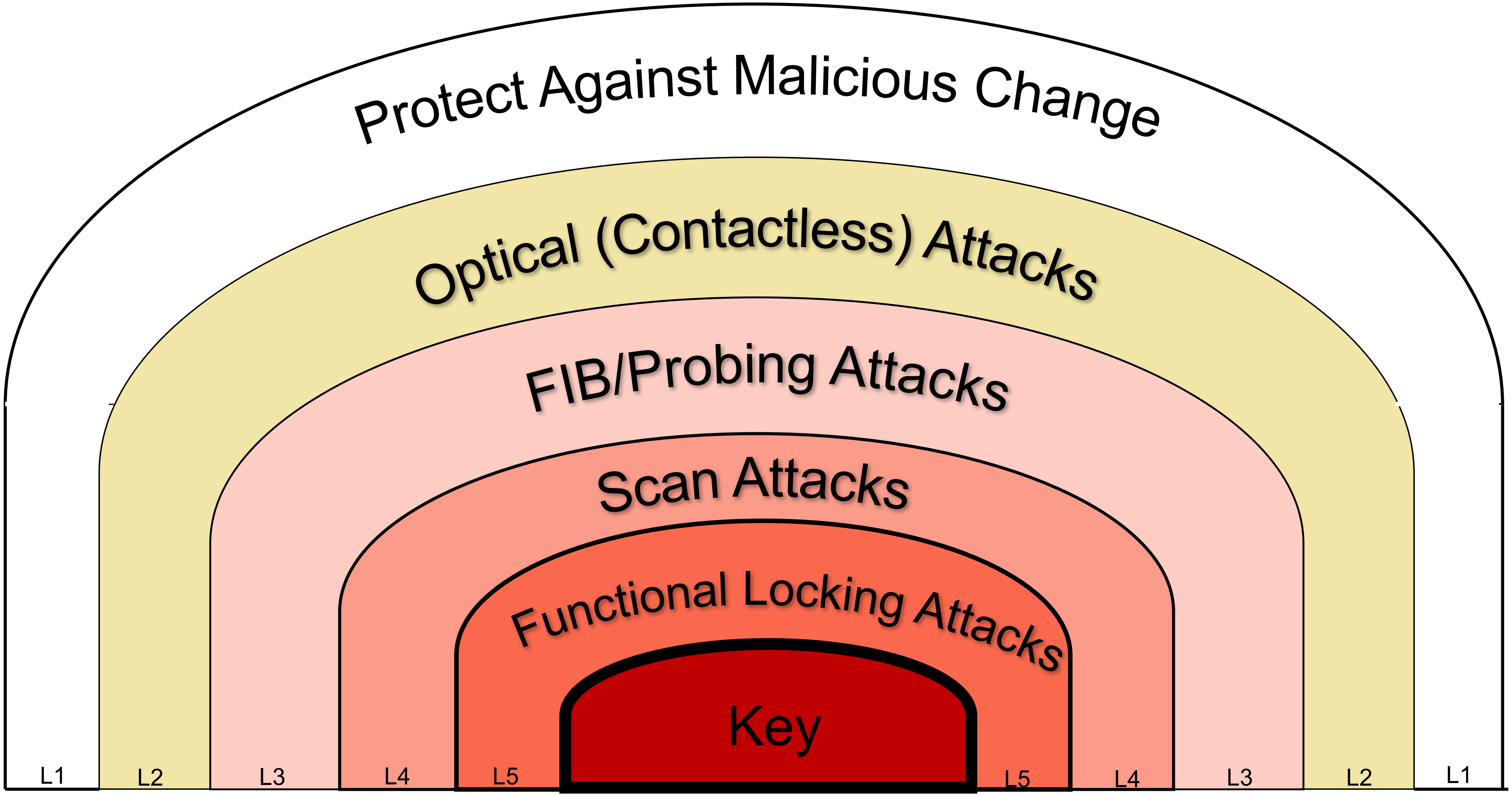


A number of vulnerabilities must be addressed to make **logic locking** a viable technology

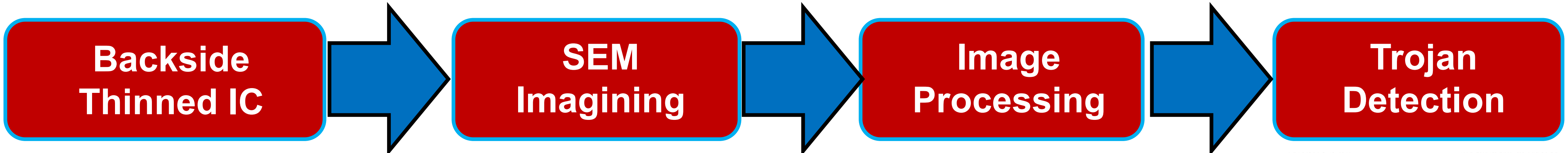
Defense-in-Depth

To defend a system against any particular attack using several independent methods

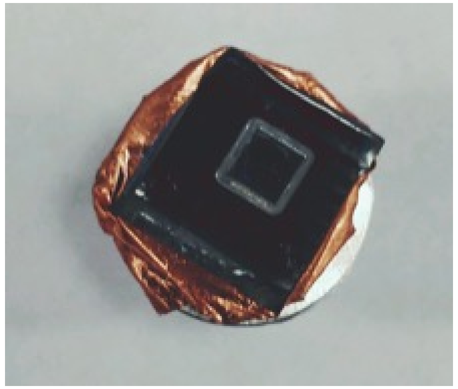
Defense-in-Depth for Protecting Obfuscation

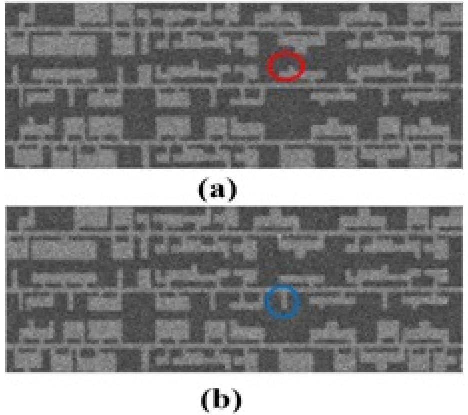

Protect Against Malicious Change
Optical (Contactless) Attacks
FIB/Probing Attacks
Scan Attacks
Functional Locking Attacks
Key
L1
L2
L3
L4
L5
L5
L4
L3
L2
L1

Layer 1: Trojan Scanner



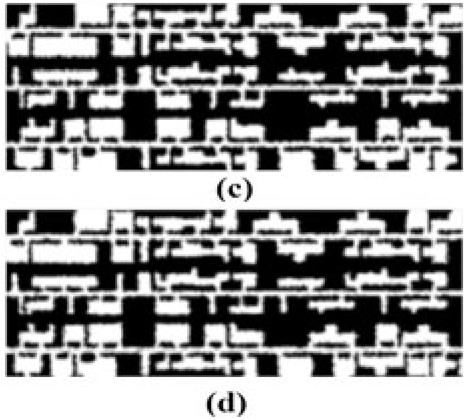
Backside Thinned IC → SEM Imagining → Image Processing → Trojan Detection





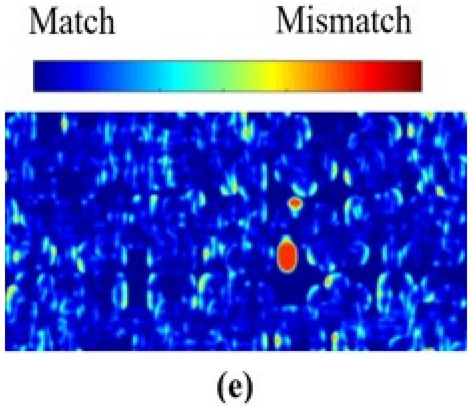
(a)

(b)



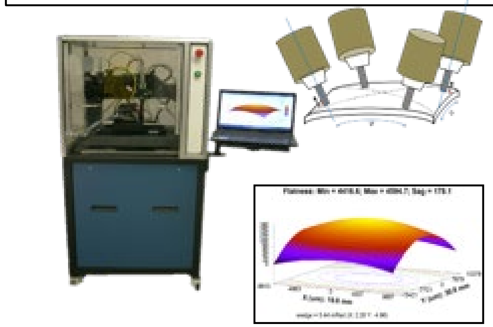
(c)

(d)



(e)

- Outer package removal.
- Chemical de-capsulation
- Backside thinning ~ 0um



Setting Parameters

i. High Voltage (HV)
ii. Dwelling time (Speed)
iii. Field of View (FoV) / (Magnification)
iv. Resolution

Capturing Images

(a) IC Under Auth. (IUA)

Image Registration

- Noise Removal - FFT BP filter
- Binarization - Adaptive Thresholding
- Smoothening - Gaussian Filter
- Flood Fill

Detection

- Optimized - **S**tructural **SIM**ilarity Index (SSIM) algorithm.
- Threshold based image labelling of suspicious areas of chip.

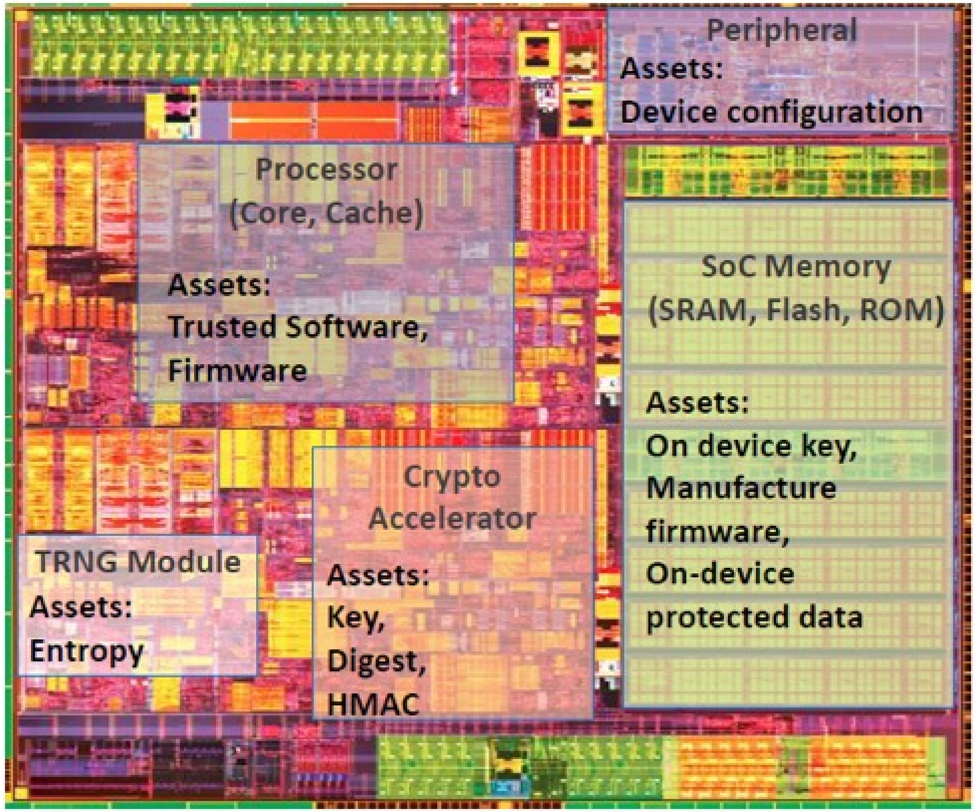
Protect Assets

Security Assets

Asset: A resource of value worth protecting from an adversary

Security Assets in SoCs:

- On-device keys (developer/OEM)
- Device configuration
- Manufacturer Firmware
- Application software
- On-device sensitive data
- Communication credentials
- Random number or entropy
- E-fuse,
- PUF, and more…



Source: Intel

Protect Assets: Strong Algorithms, Weak Implementation

Strong Algorithm & Architecture

Weak Implementation & Execution

Algorithms, architectures, and policies could be impacted by design methods that do not understand Security!

Vulnerabilities

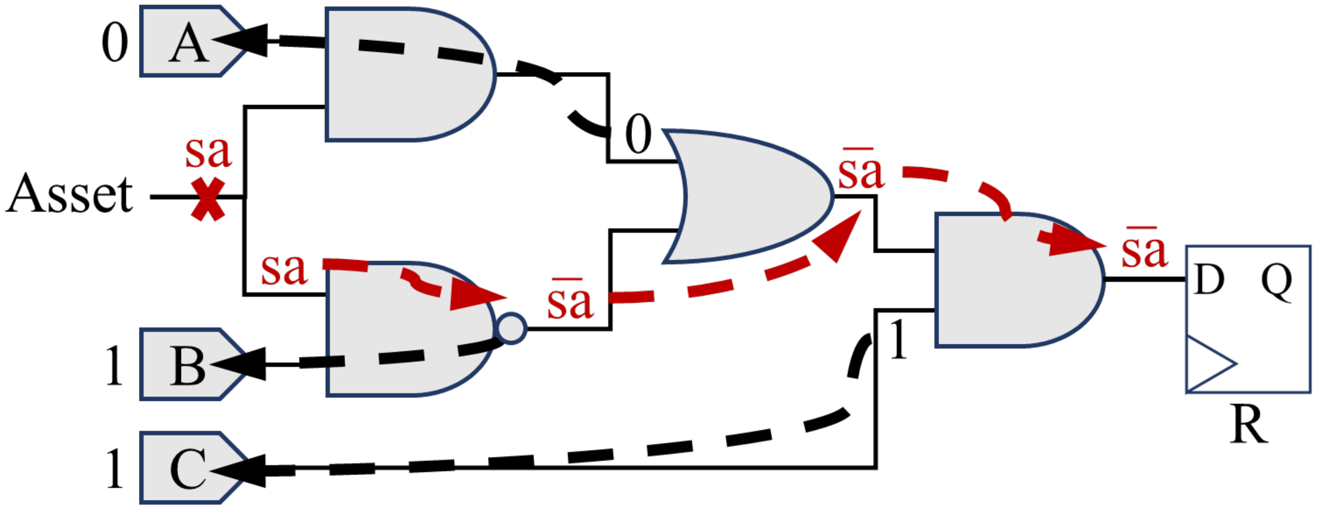
- Information Leakage
- Side Channel Leakage
- Fault Injection
- IP Tampering, Trojan Insertion

Accesses/attack surfaces

- Remote Access (E.g., WiFi, Ethernet, Zigbee, etc.)
- PCB Access (E.g., JTAG and Debug ports)
- Physical Access

Gate Level -- Information Leakage

- Modeling an asset as **a stuck at fault**
- Utilize automatic test pattern generation algorithms to detect that fault
- A **successful** detection → Existence of information flow



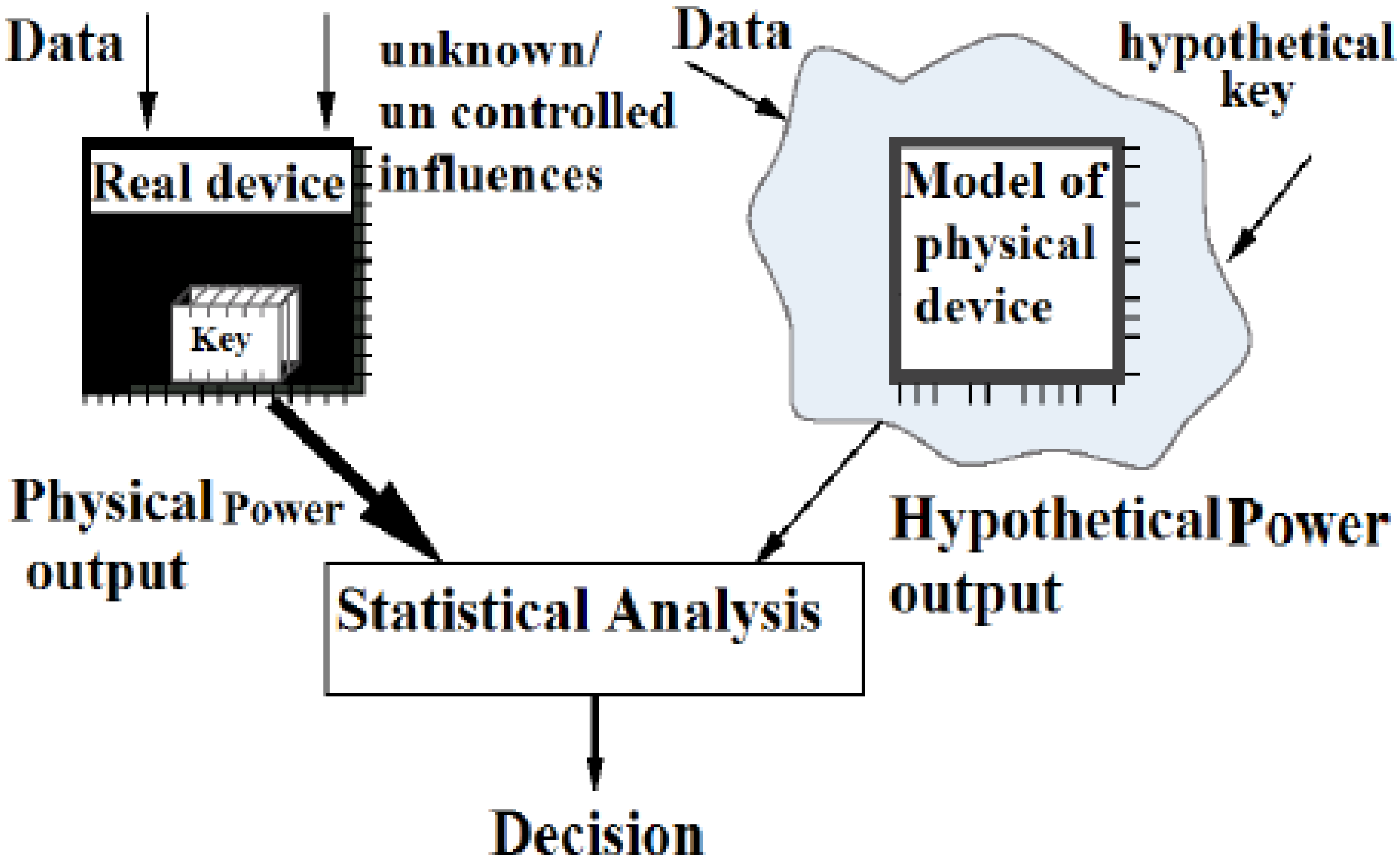
We need to identify all observe points → Asset can be observed

Confidentiality Analysis

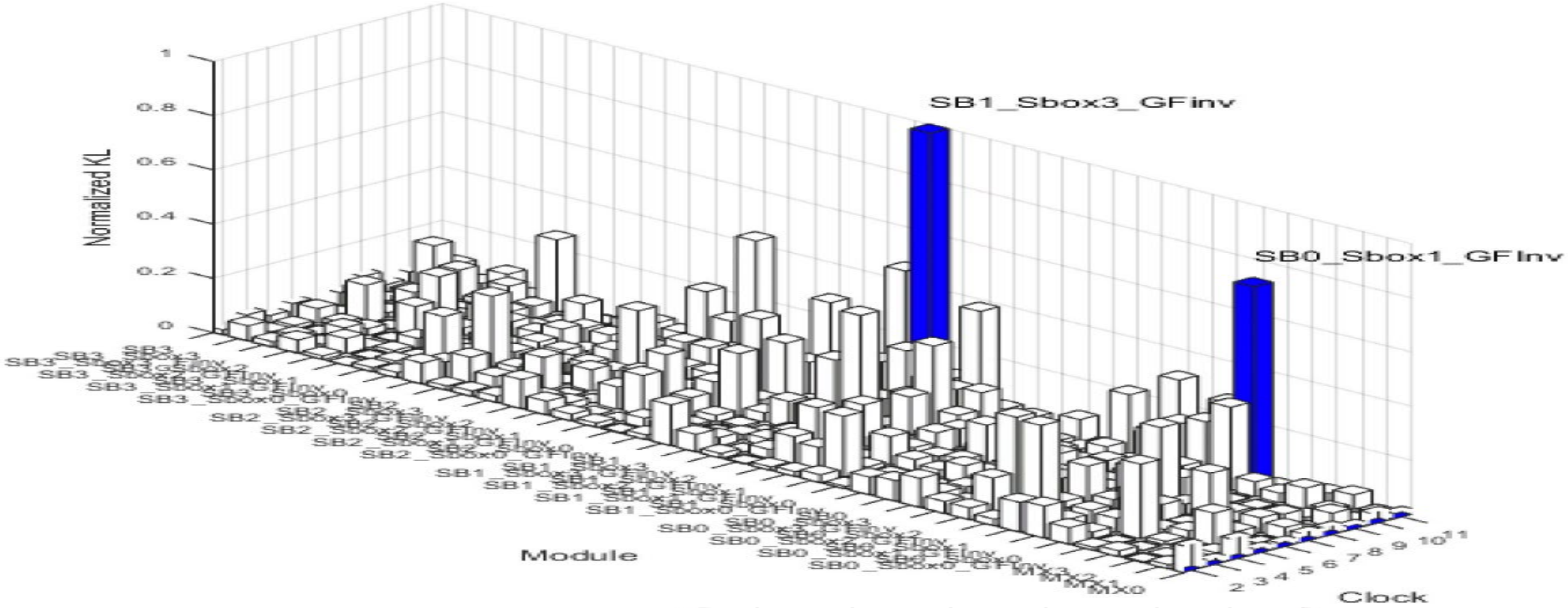
Encryption Algorithm	Design	Seq. Elements	Observable Points	Distance		Stimulus	
				Min	Max	Min	Max
AES	high speed	10769	2	2	3	5	7
	small area	2575	4	2	2	6	6
	ultra-high speed	6720	2	0	1	2	3
Single-DES	small area	64	32	11	15	15	17
Triple-DES	small area	128	48	10	12	29	33
	high speed	8808	2	2	2	3	3
RSA	basic	555	32	4	3	6	6
PRESENT	light ware	149	2	2	2	3	3

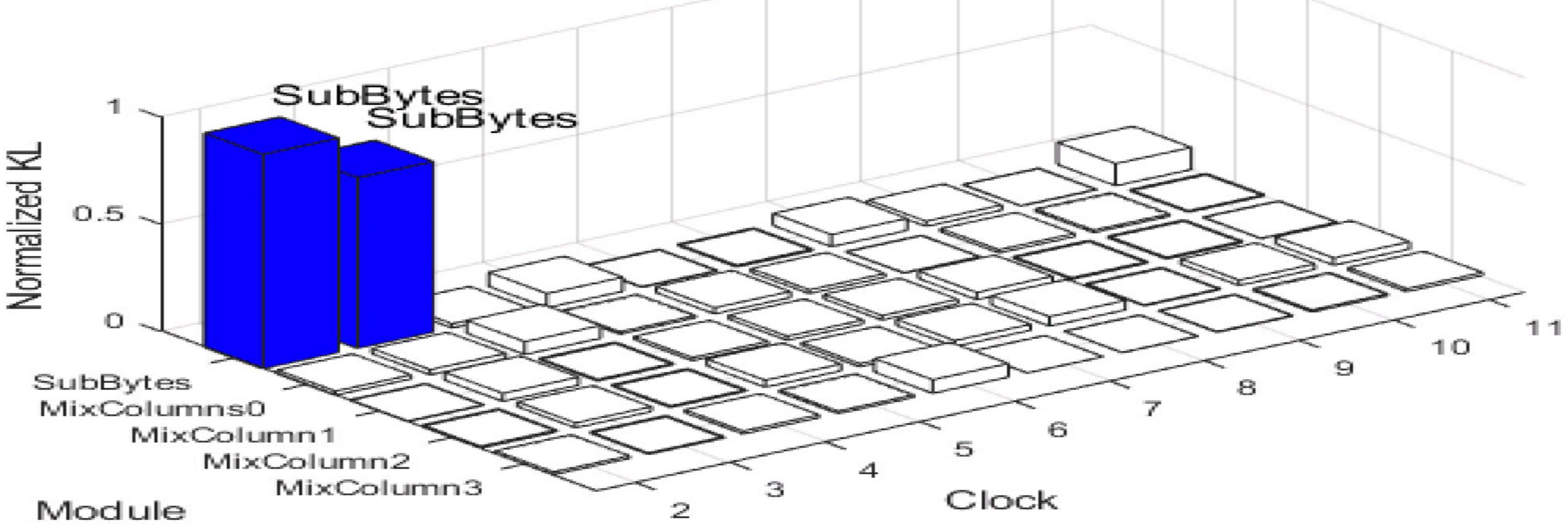
- **Takeaways**
  - All implementation of AES, RSA and PRESENT encryption modules **have vulnerability due to DFT insertion**
  - The ‘Distance’ and ‘Stimulus’ → quantitative measure of vulnerability
  - **Higher** value → less vulnerable

Power Side Channel Attacks

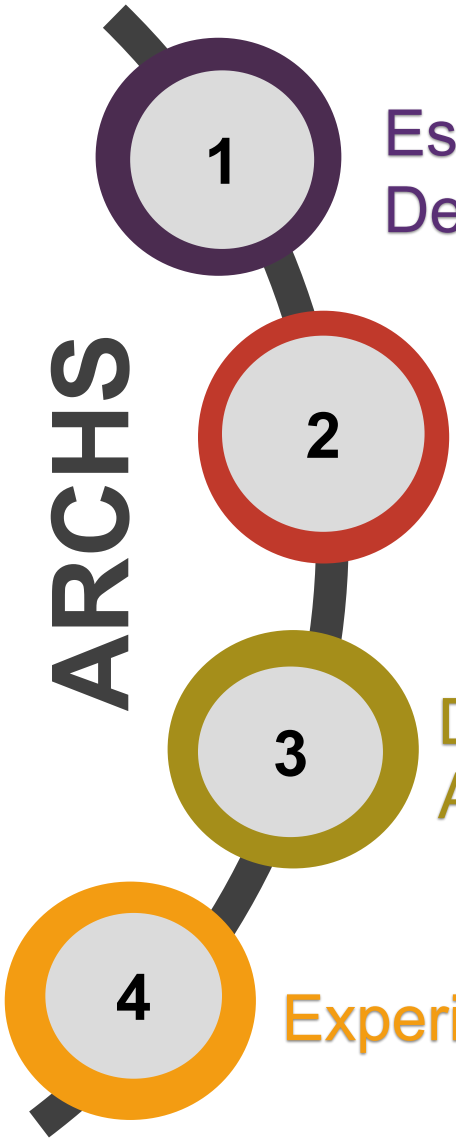


Block Leakage Analysis





Security Rule Check

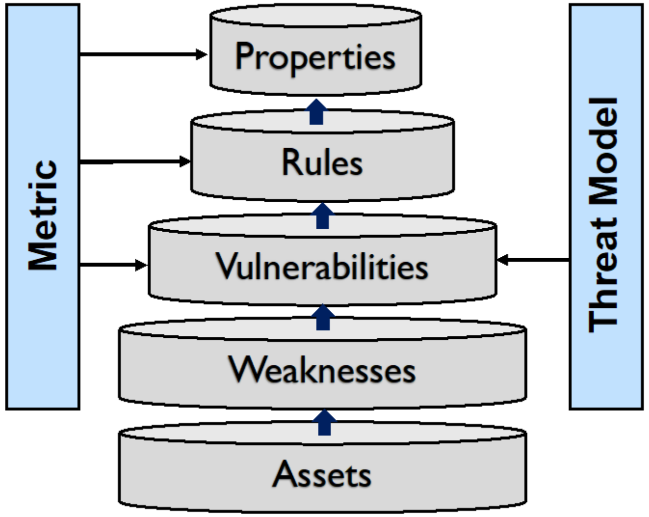


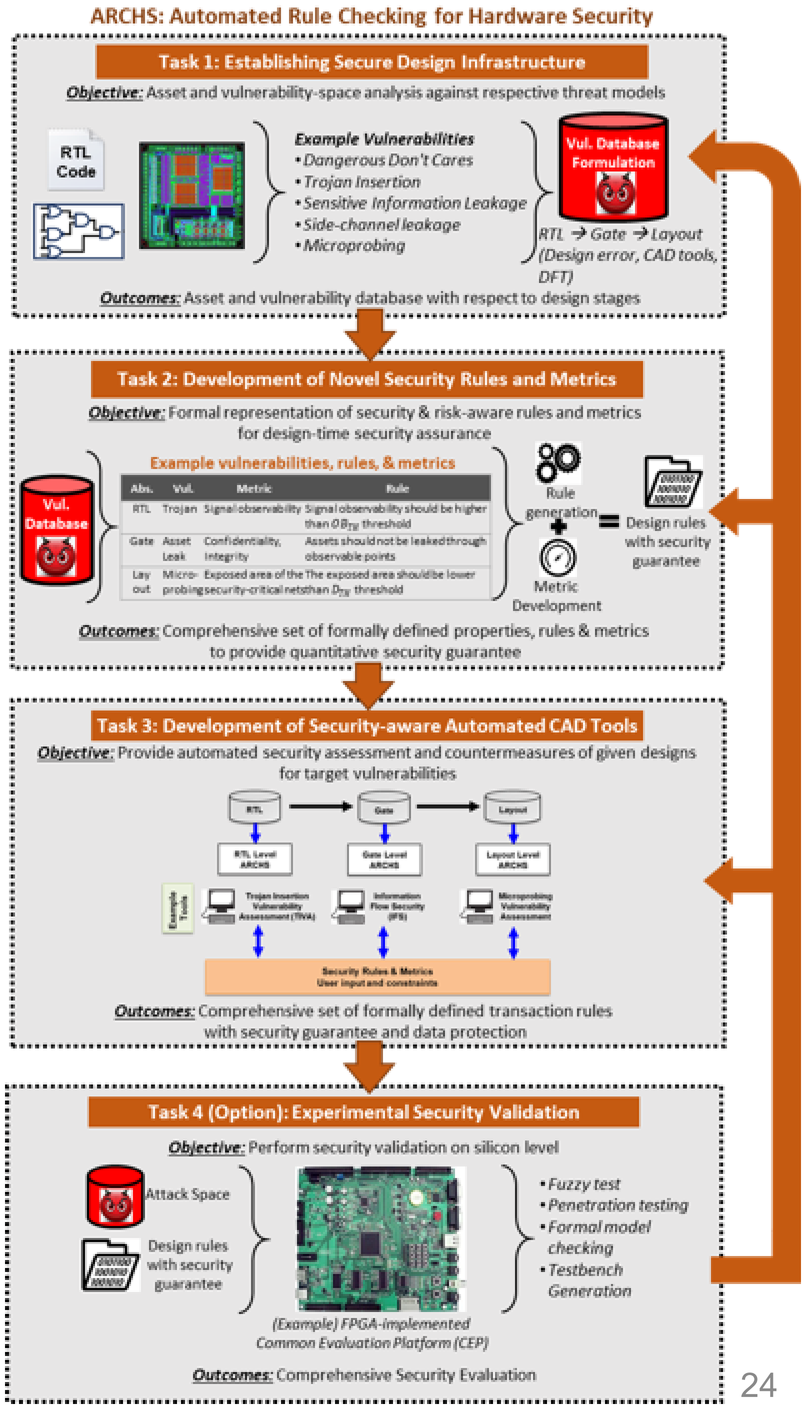
Establishing Secure Design Infrastructure

Development of Security Rules and Metrics

Development of Security-aware Automated CAD Tools

Experimental Security Validation




ARCHS: Automated Rule Checking for Hardware Security

Task 1: Establishing Secure Design Infrastructure

Objective: Asset and vulnerability-space analysis against respective threat models

Example Vulnerabilities
- *Dangerous Don't Cares*
- *Trojan Insertion*
- *Sensitive Information Leakage*
- *Side-channel leakage*
- *Microprobing*

Outcomes: Asset and vulnerability database with respect to design stages

Task 2: Development of Novel Security Rules and Metrics

Objective: Formal representation of security & risk-aware rules and metrics for design-time security assurance

Example vulnerabilities, rules, & metrics

Abs.	Vul.	Metric	Rule
RTL	Trojan	Signal observability	Signal observability should be higher than OB_{TH} threshold
Gate	Asset Leak	Confidentiality, Integrity	Assets should not be leaked through observable points
Lay out	Micro-probing	Exposed area of the security-critical nets	The exposed area should be lower than D_{TH} threshold

Outcomes: Comprehensive set of formally defined properties, rules & metrics to provide quantitative security guarantee

Task 3: Development of Security-aware Automated CAD Tools

Objective: Provide automated security assessment and countermeasures of given designs for target vulnerabilities

RTL
Gate
Layout
RTL Level ARCHS
Gate Level ARCHS
Layout Level ARCHS
Example Tools
Trojan Insertion Vulnerability Assessment (TIVA)
Information Flow Security (IFS)
Microprobing Vulnerability Assessment
Security Rules & Metrics
User input and constraints

Outcomes: Comprehensive set of formally defined transaction rules with security guarantee and data protection

Task 4 (Option): Experimental Security Validation

Objective: Perform security validation on silicon level

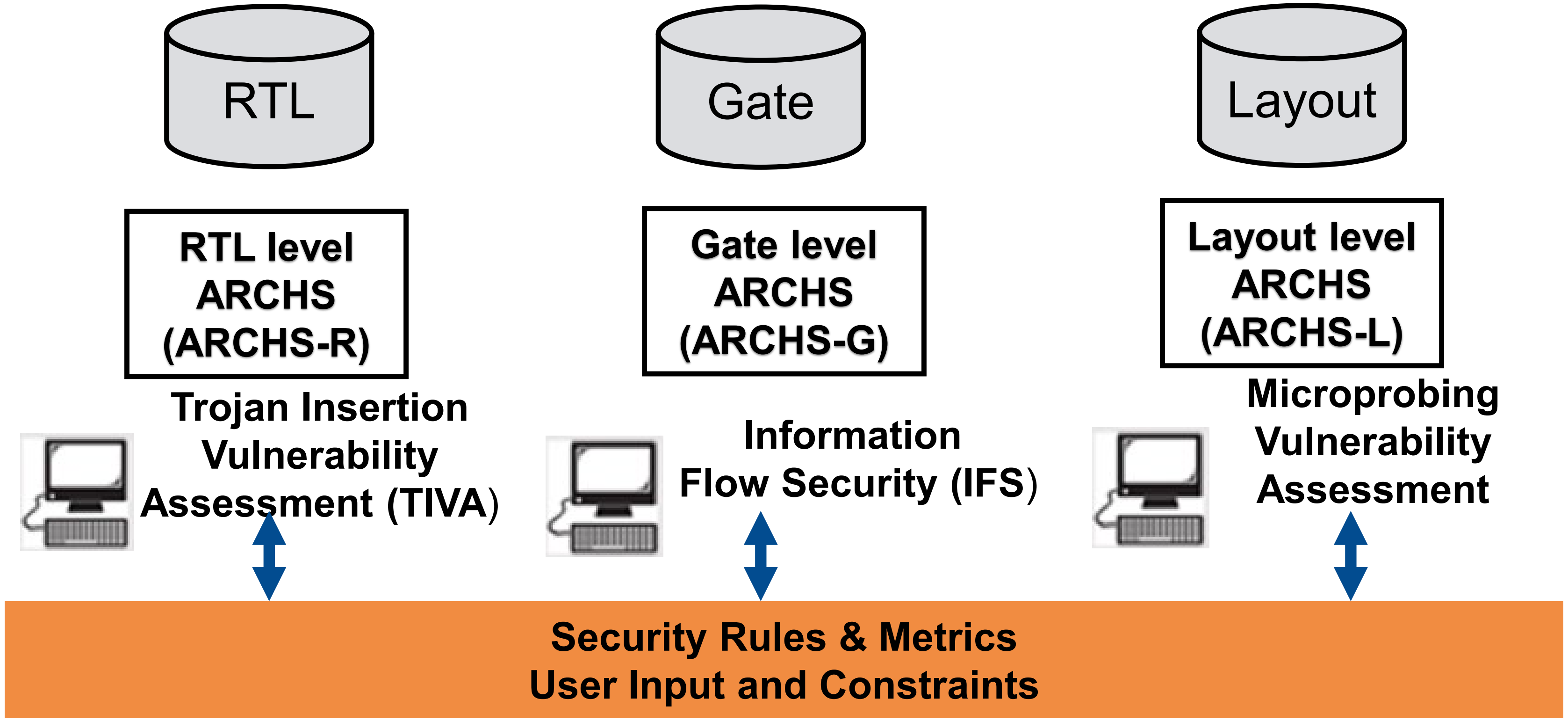
(Example) FPGA-implemented Common Evaluation Platform (CEP)

- *Fuzzy test*
- *Penetration testing*
- *Formal model checking*
- *Testbench Generation*

Outcomes: Comprehensive Security Evaluation

Security Rule Check

Objective: Provide automated security assessment and possible countermeasures of given designs for target vulnerabilities



RTL level ARCHS (ARCHS-R)

Gate level ARCHS (ARCHS-G)

Layout level ARCHS (ARCHS-L)

Trojan Insertion Vulnerability Assessment (TIVA)

Information Flow Security (IFS)

Microprobing Vulnerability Assessment

Security Rules & Metrics
User Input and Constraints

Outcomes: Comprehensive set of formally defined transaction rules with security guarantees and data protection

Chip Backside Is A New Backdoor

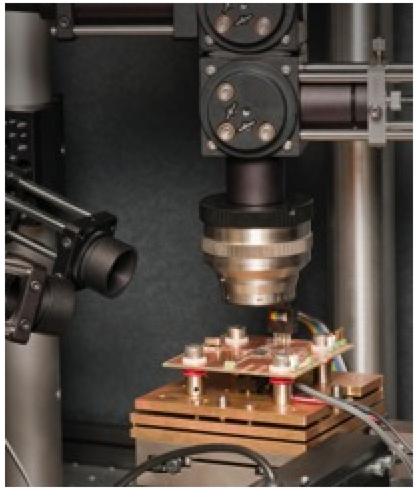
- **Frontside: Multiple interconnect layers obstruct the optical path to transistor devices**
- **Backside:** Active devices are directly accessible

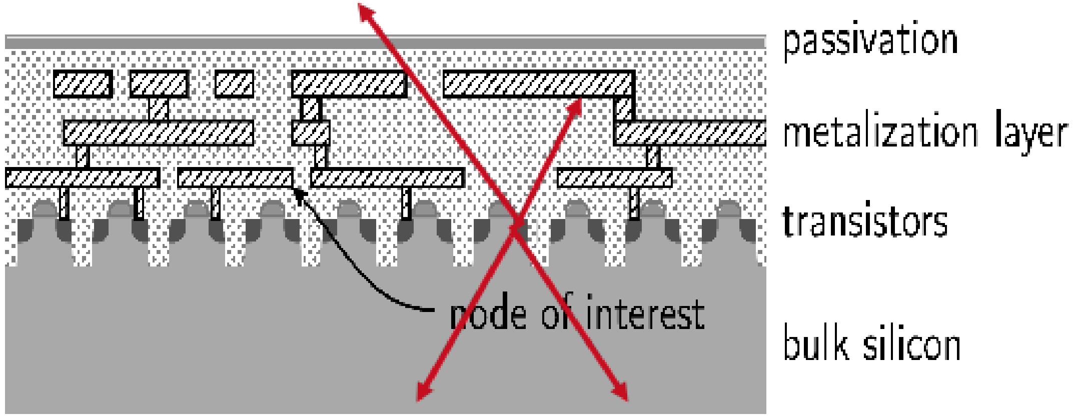
✦ **Photon Emission**

✦ **Laser Stimulation/Fault Injection**

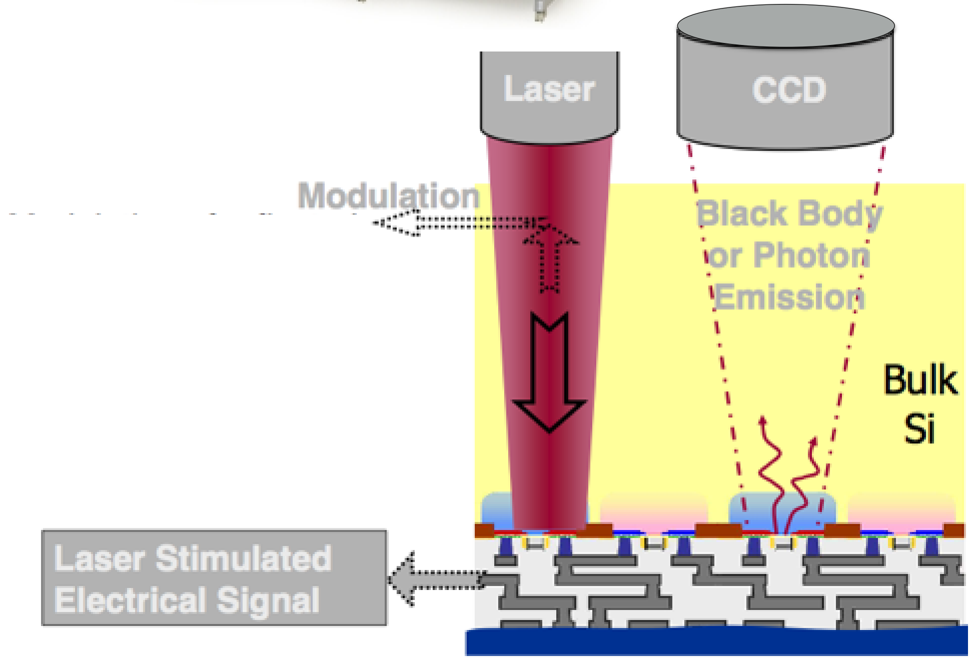
✦ **Optical Contactless Probing**

Hamamatsu PHEMOS - 1000

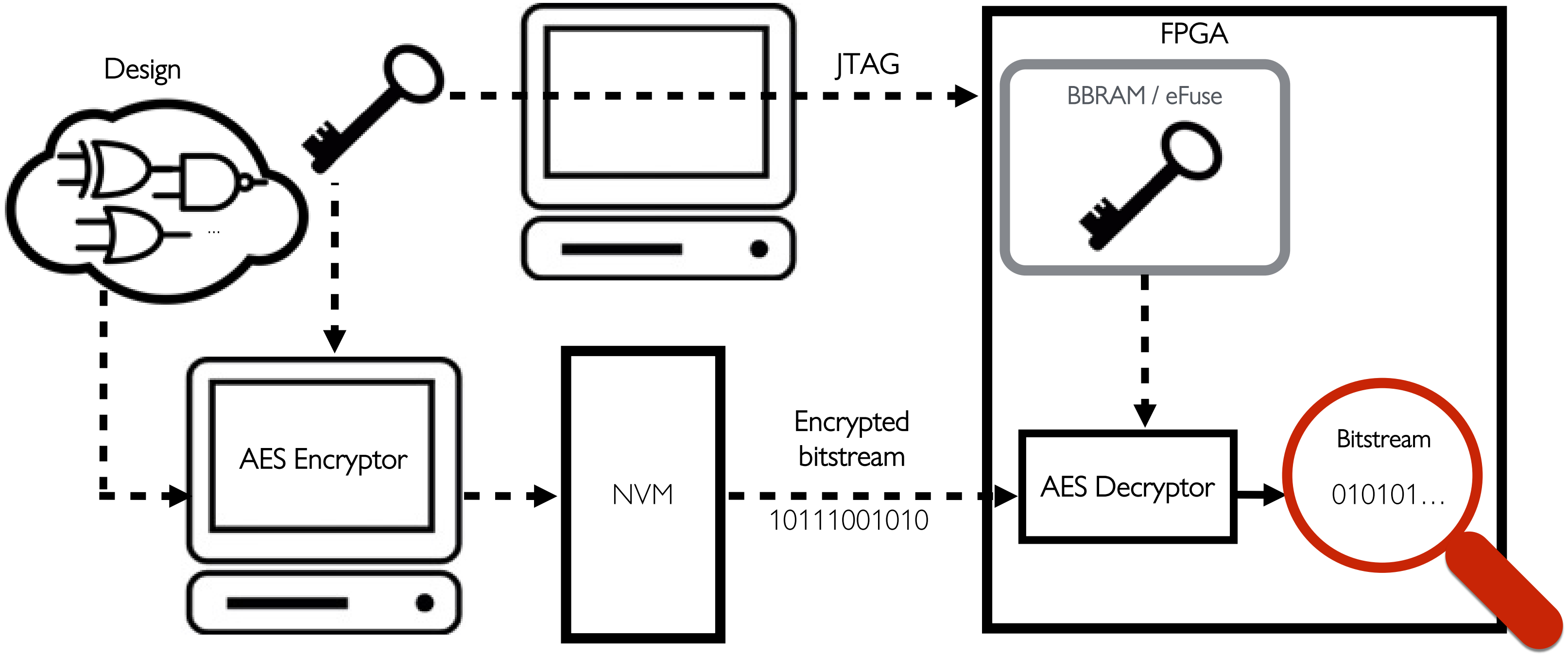


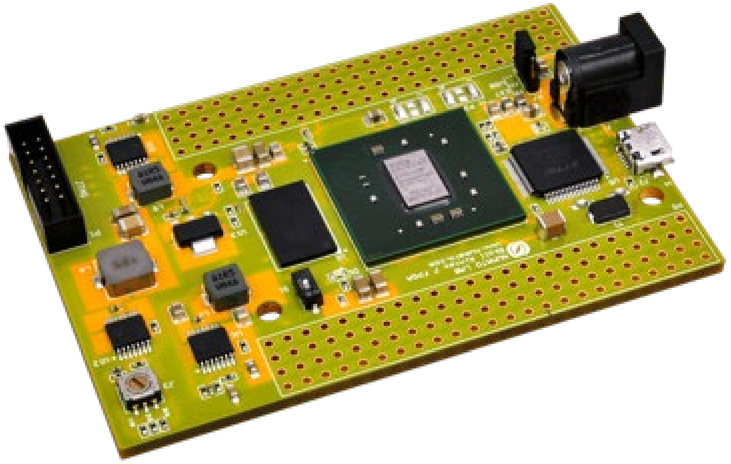


Source: C. Boit et. al.


Laser
CCD
Modulation
Black Body or Photon Emission
Bulk Si
Laser Stimulated Electrical Signal

Attacking Bitstream Encryption of FPGAs





- Device under Test (DUT): Xilinx Kintex 7 development board
  - Chip's technology: 28 nm
  - No chip preparation (e.g., depackaging, silicon polishing, etc.)
- Optical Setup: Hamamatsu PHEMOS-1000
  - Laser wavelength: 1.3 μm
  - Laser spot size: >1 μm

- Non-destructive
- Non-invasive
- No Footprint

Localizing the Configuration Logic

Xilinx Kintex 7 in flip-chip package

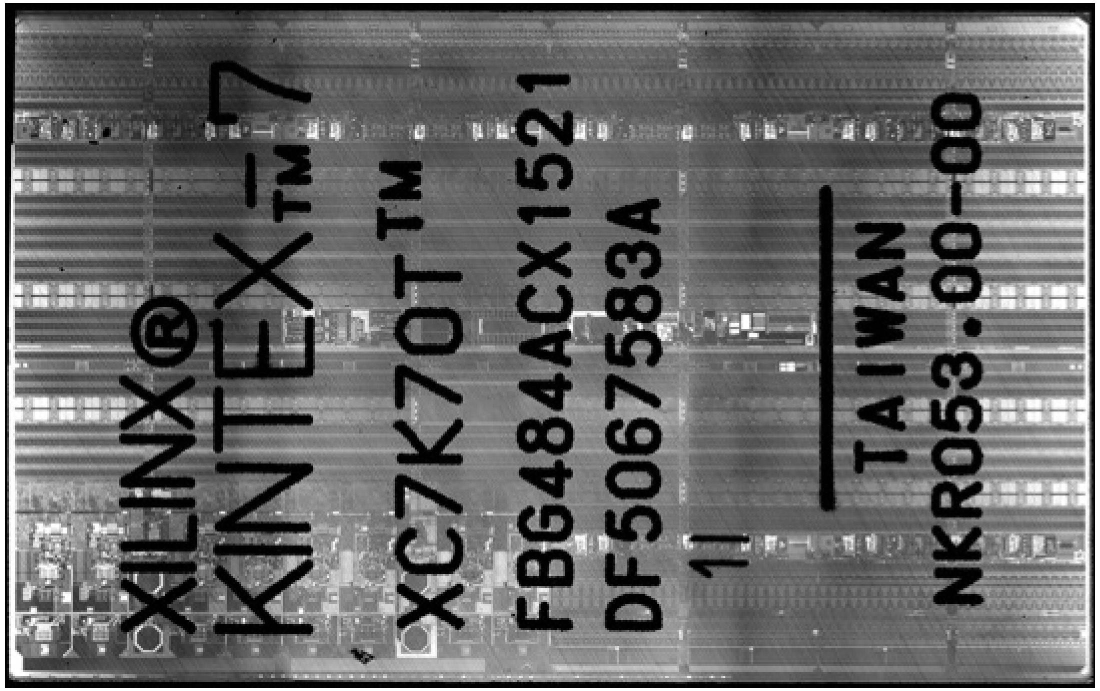
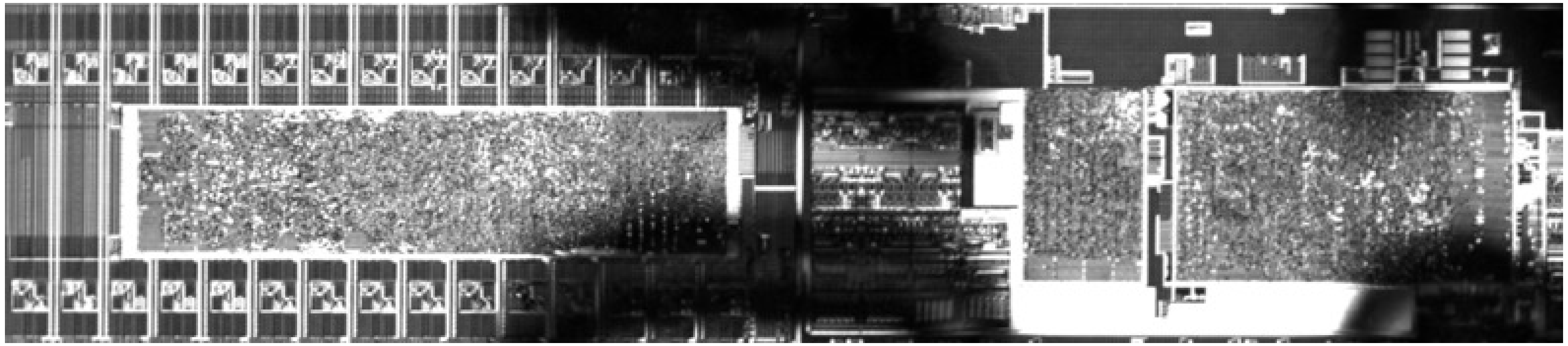


Image acquisition with a infra-red laser scanning microscope

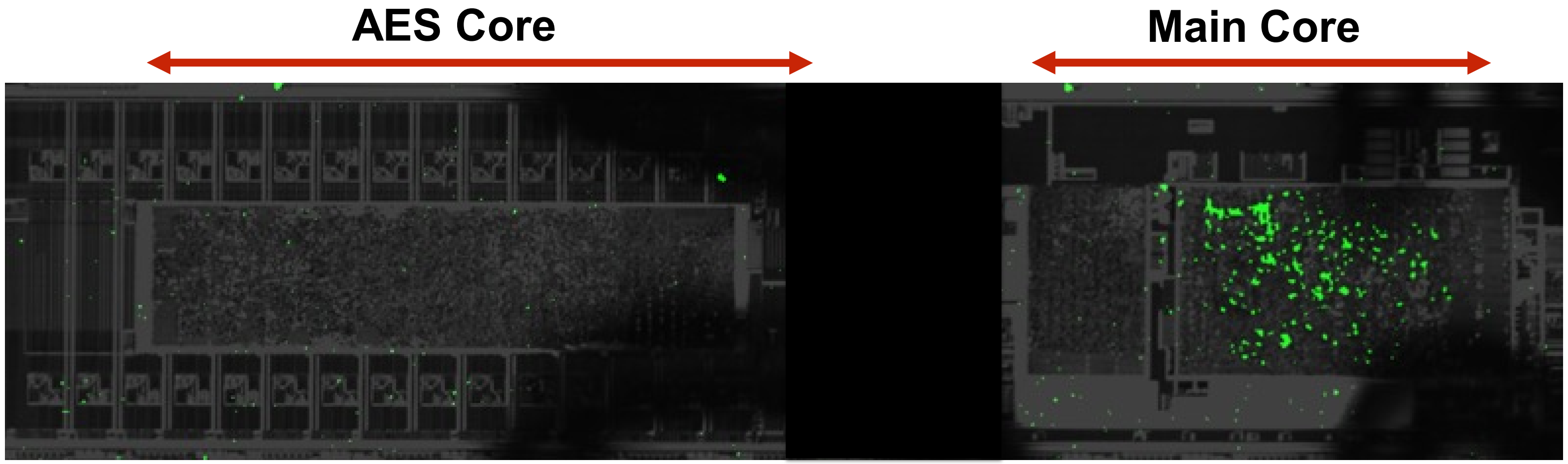
Tajik, S., Lohrke, H., Seifert, J. P., & Boit, C. "**On the Power of Optical Contactless Probing: Attacking Bitstream Encryption of FPGAs**," In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security.

Localizing the Configuration Logic



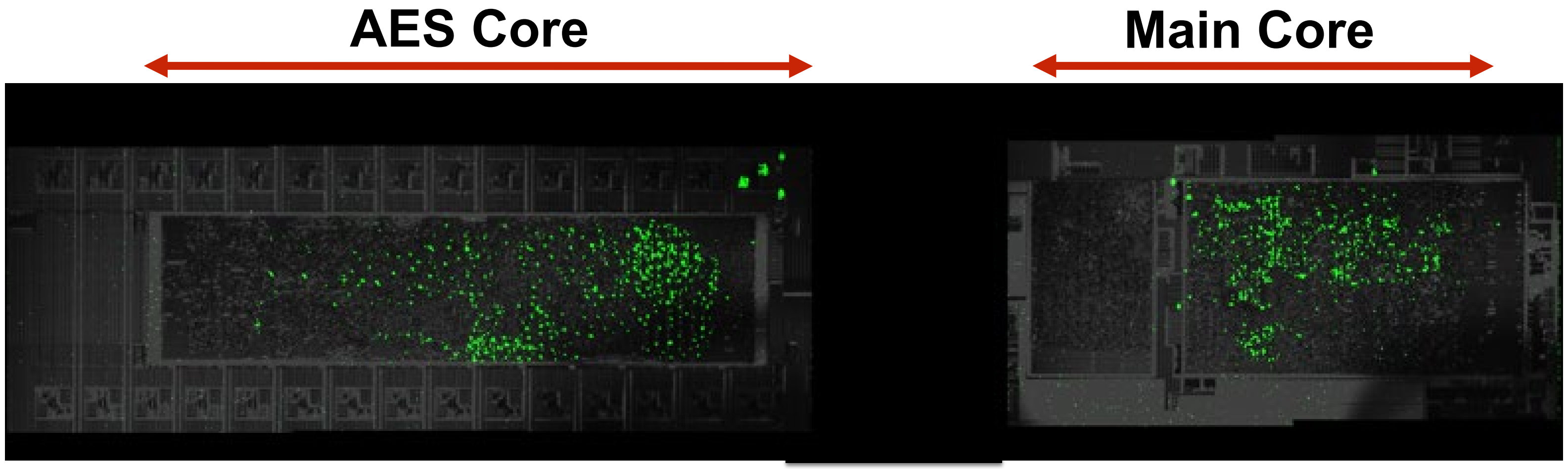
Random Logic

Localizing Decryption Core using EOFM



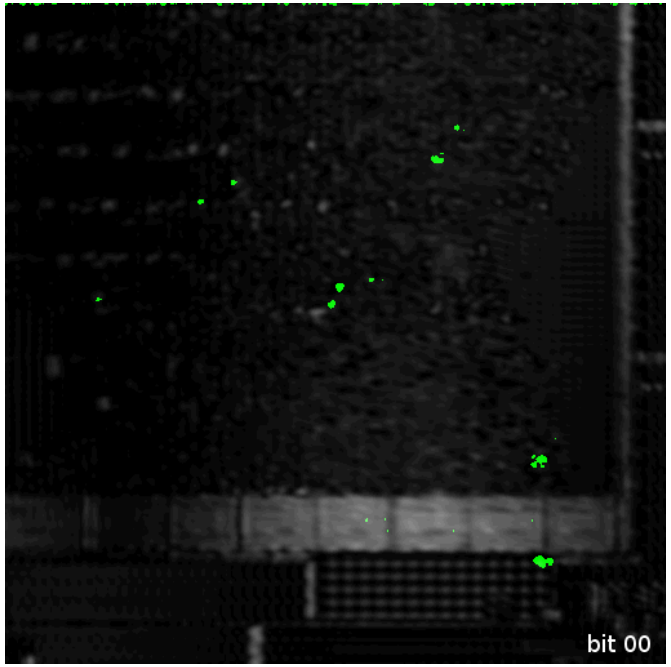
Clock activity for unencrypted bitstream

Localizing Decryption Core using EOFM



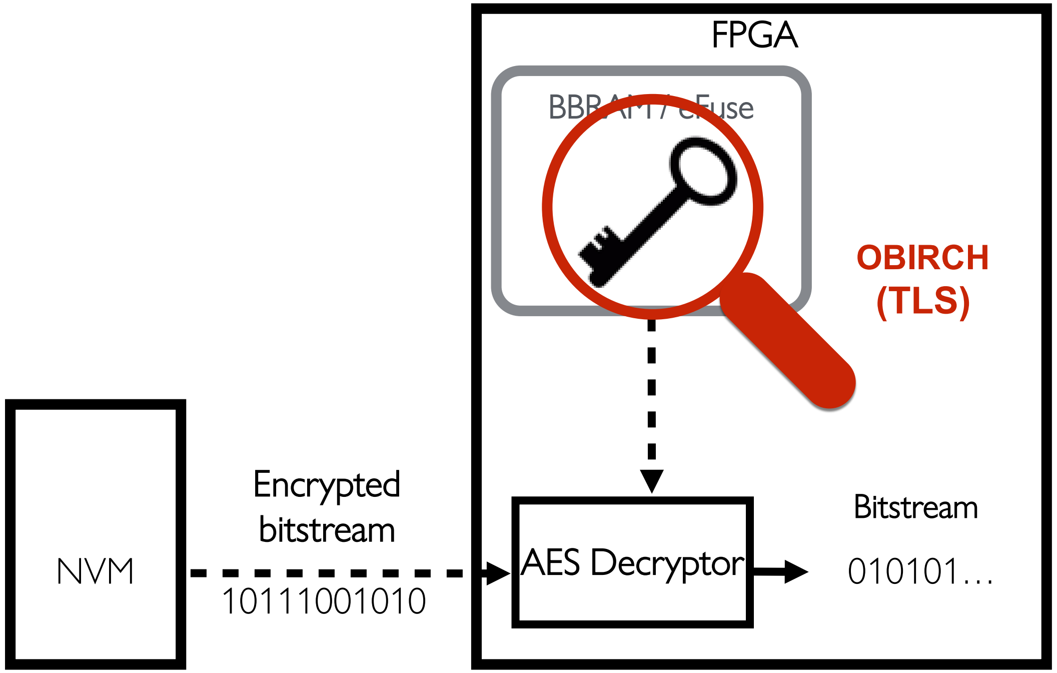
Clock activity for encrypted bitstream

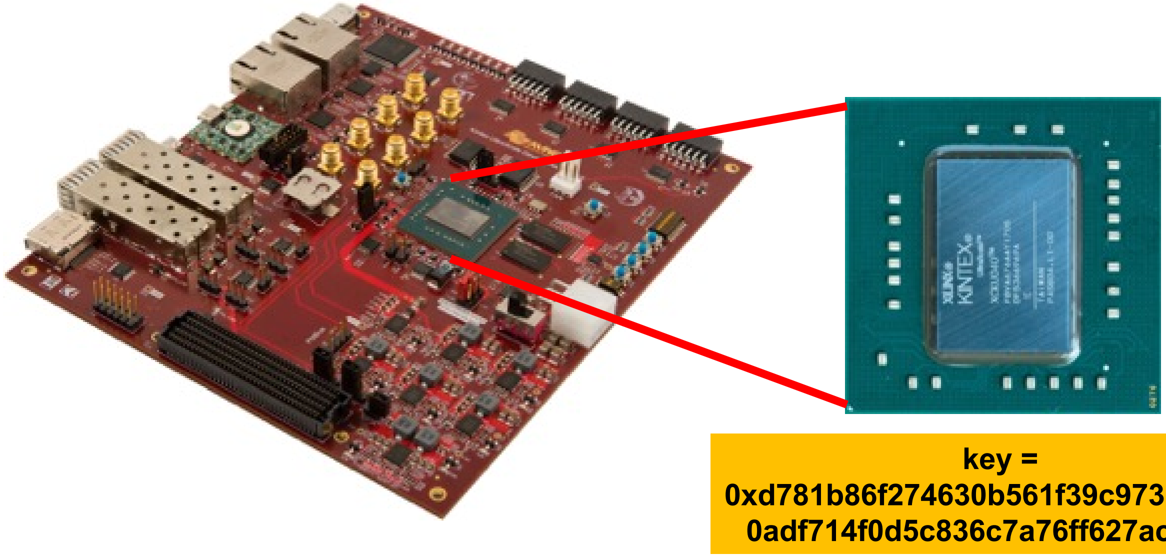
Locating the plaintext data



Locations in AES output port

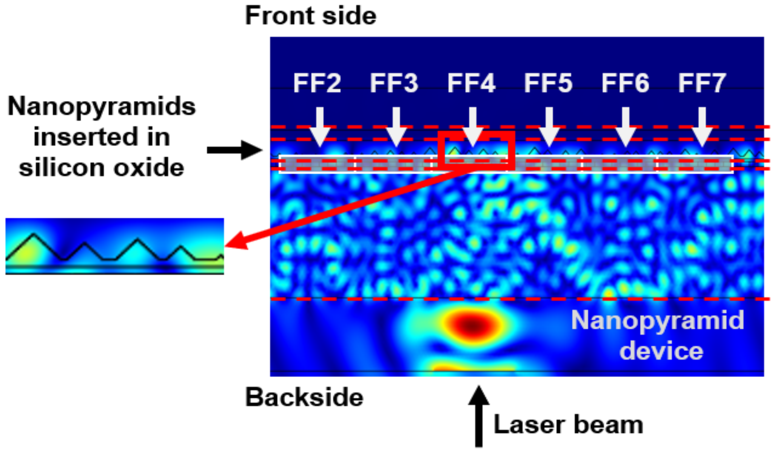
Key Extraction

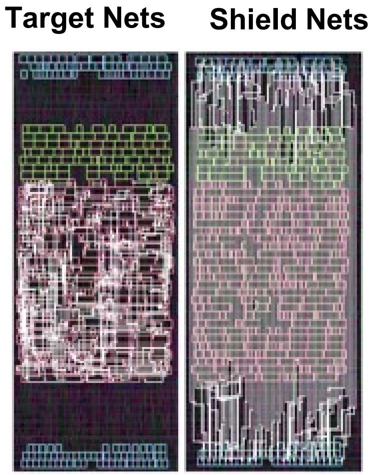




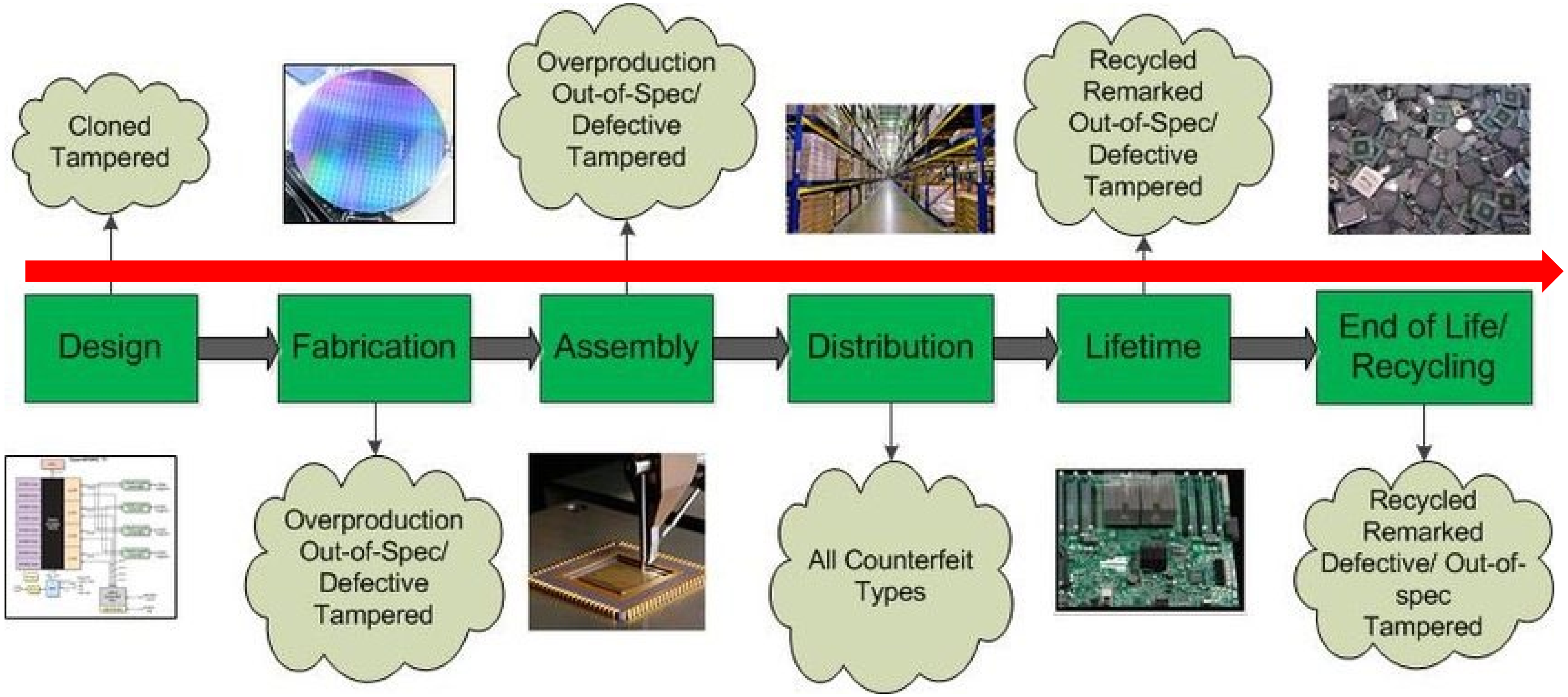
key =
0xd781b86f274630b561f39c9736f512eb
0adf714f0d5c836c7a76ff627aca4923

- **Protection**
  - **Circuit Level Solutions**
  - **Device Level solutions**
  - **Material Level Solutions**





Protect the Supply Chain



Design

Cloned
Tampered

Fabrication

Overproduction
Out-of-Spec/
Defective
Tampered

Assembly

Overproduction
Out-of-Spec/
Defective
Tampered

Distribution

All Counterfeit Types

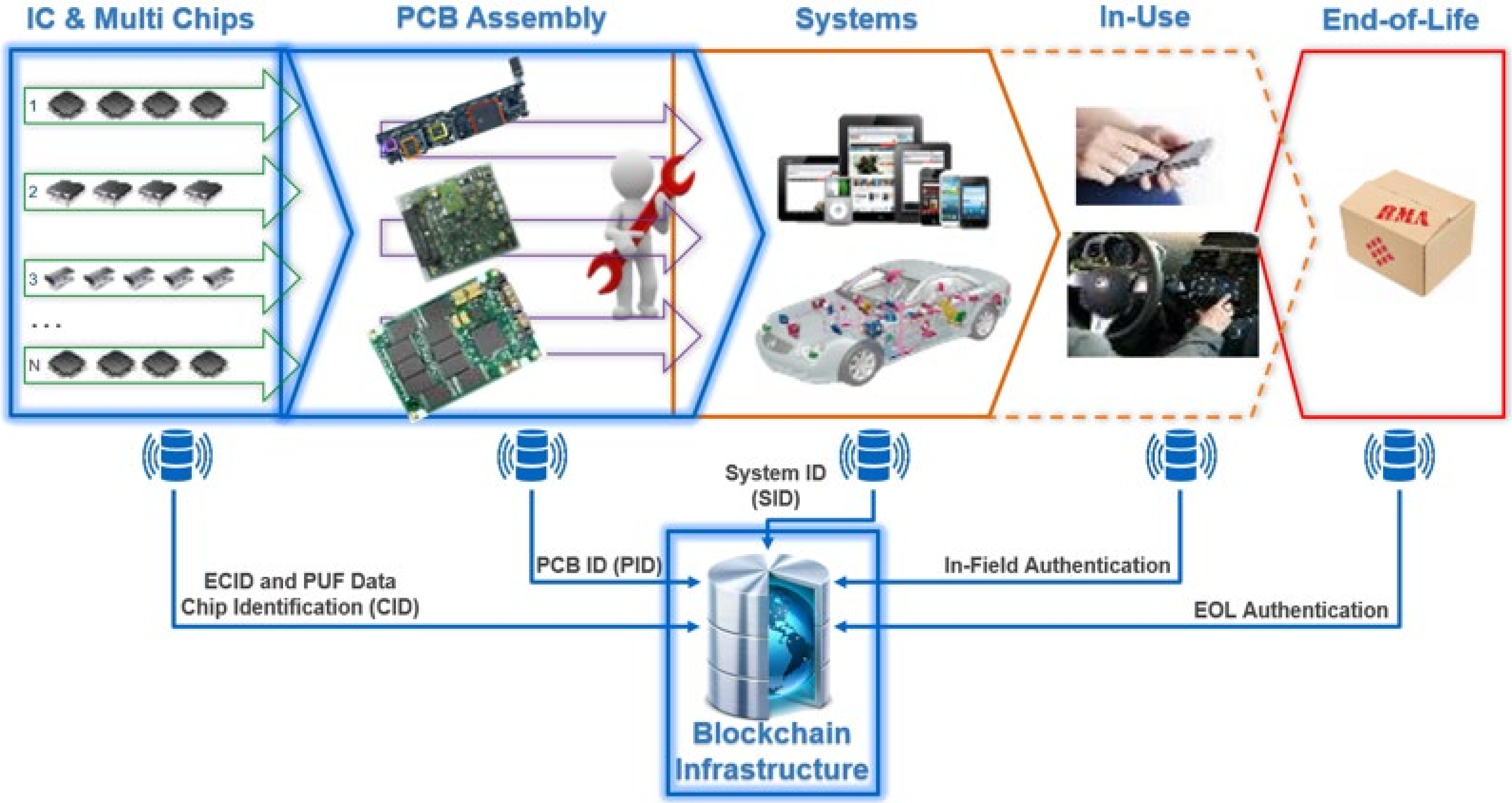
Lifetime

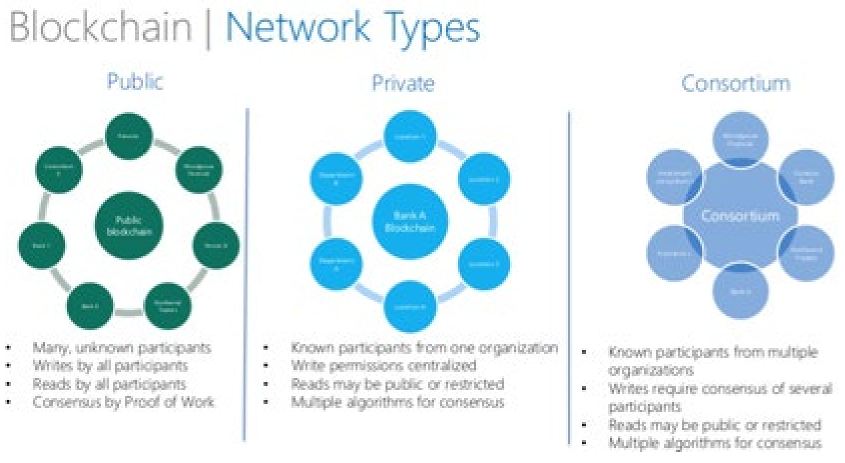
Recycled
Remarked
Out-of-Spec/
Defective
Tampered

End of Life/ Recycling

Recycled
Remarked
Defective/ Out-of-spec
Tampered

Device-to-System





Public

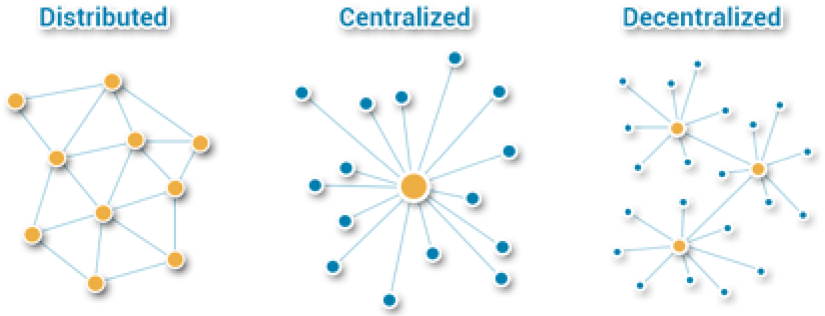
- Many, unknown participants
- Writes by all participants
- Reads by all participants
- Consensus by Proof of Work

Private

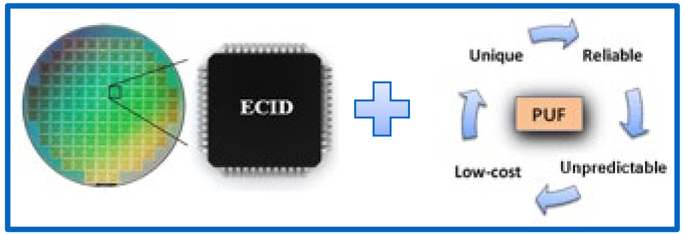
- Known participants from one organization
- Write permissions centralized
- Reads may be public or restricted
- Multiple algorithms for consensus

Consortium

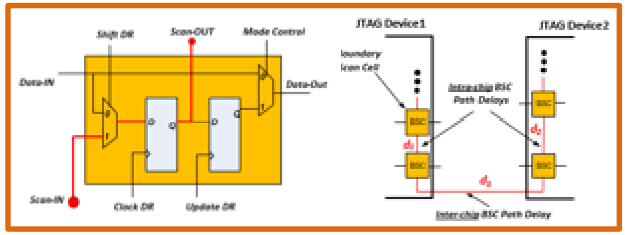
- Known participants from multiple organizations
- Writes require consensus of several participants
- Reads may be public or restricted
- Multiple algorithms for consensus



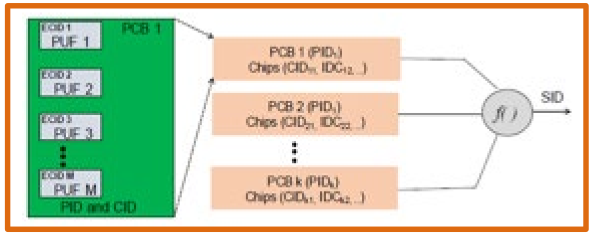
IC Authentication



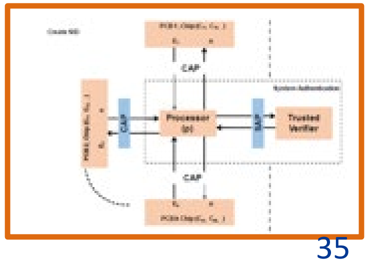
PCB Authentication



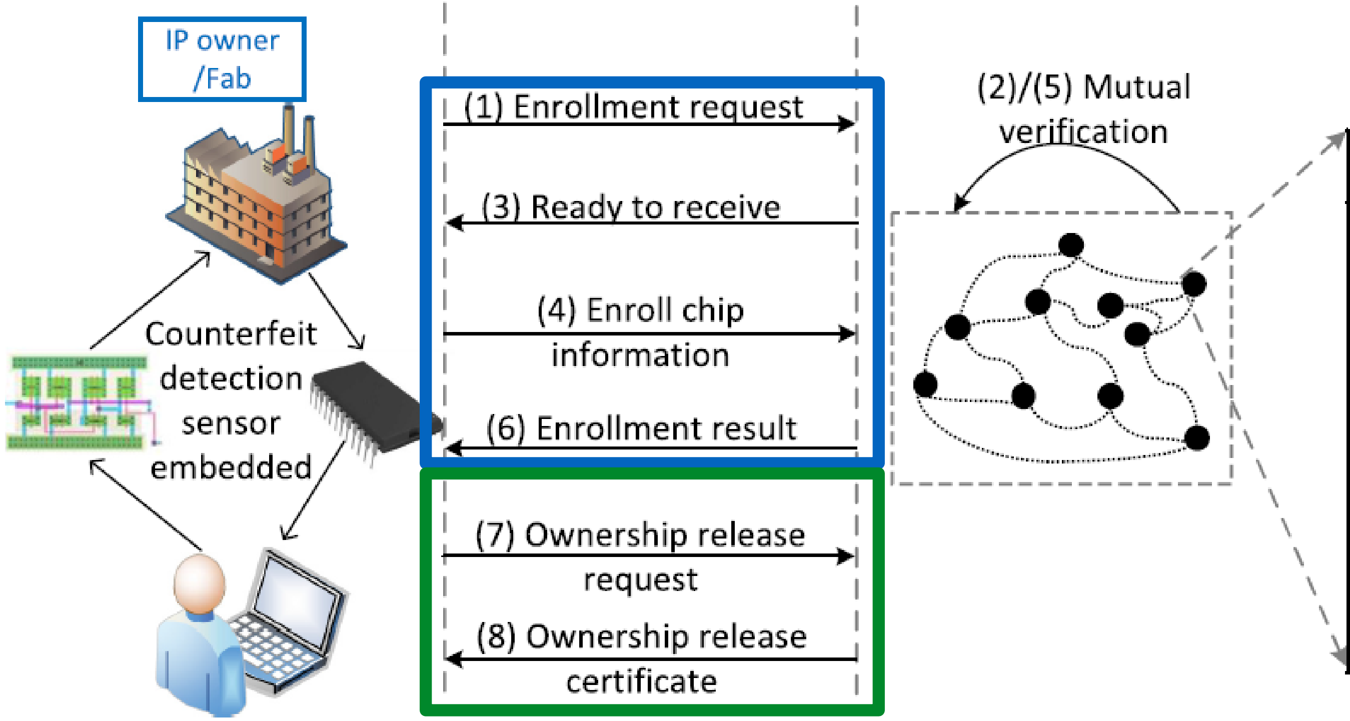
Subsystem Authentication



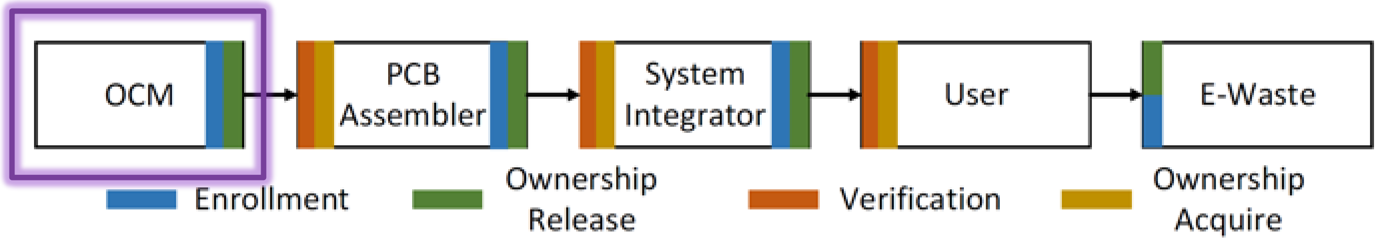
Hardware & Firmware Self Authentication



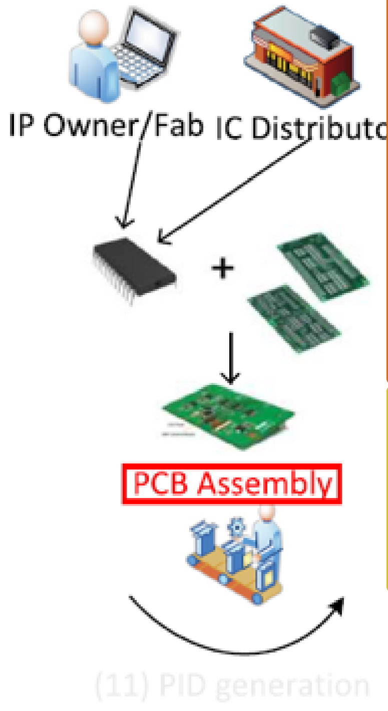
OCM: Enrollment & Ownership Release


IP owner /Fab
Counterfeit detection sensor embedded
(1) Enrollment request
(3) Ready to receive
(4) Enroll chip information
(6) Enrollment result
(7) Ownership release request
(8) Ownership release certificate
(2)/(5) Mutual verification

(6)	(6)	(6)			(3)	(6)
Marking	ECID	CRPs	PID	SID	Trans. time	Stage
VM952A CCLAL59 02VLA	0000 0158 2AB3 9EAF	1011 0010 0001 1011	null	null	Jun/03/2017/ 11:30:21AM	IP owner /Fab



PCB Assembler: Verification & Ownership Acquire



(1) Verification request

(3) Ready to respond

(4) Send public information of chips

(6) Authentic/Counterfeit

(7) Full verification based on CRPs

(8) Verification result

(9) Ownership acquire request

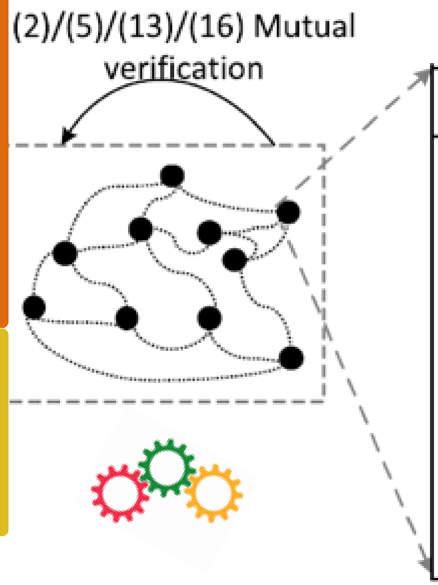
(10) Ownership release information

(12) PID enrollment request

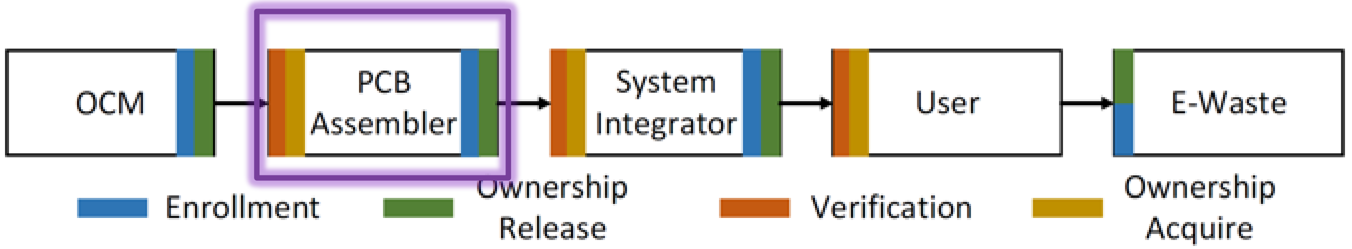
(14) Ready to receive

(15) PID enrollment

(17) PID enrollment result



(4)		(7)	(15)		(6)(16)	(6)
Marking	ECID	CRPs	PID	SID	Trans. time	Stage
VM952A CCLAL59 02VLA	0000 0158 2AB3 9EAF	1011 0010 0001 1011	null	null	Jun/03/2017/ 11:30:21AM	IP owner /Fab
					Jun/08/2017/ 09:05:21PM	PCB Assembly

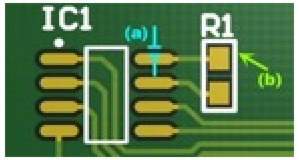


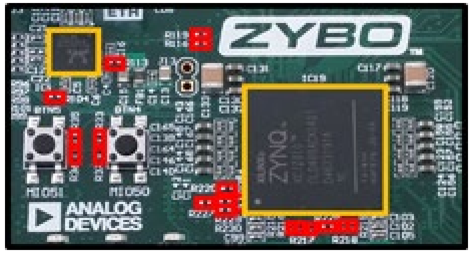
AutoBoM: External Visual Inspection of PCB

Smart phone w/ adapter

Optical Microscopy

Image Pre-processing





Bill of Material

- Chips
- Resistors
- Capacitors
- Ports

Analysis and Defect Recognition

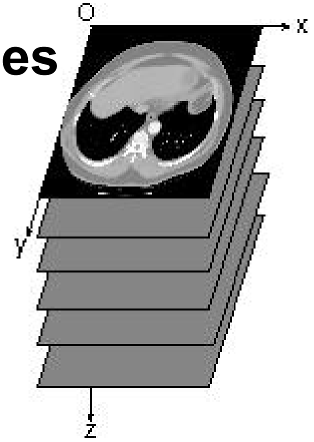
- Chips
- Discrete Components
- Solder
- Contacts
- PCB

Intelligent Microscopy for even lower time/cost!

Auto3D: Internal Inspection of PCB

X-ray CT

- Parameter Optimization
- Sample Preparation and Filtering



Slices

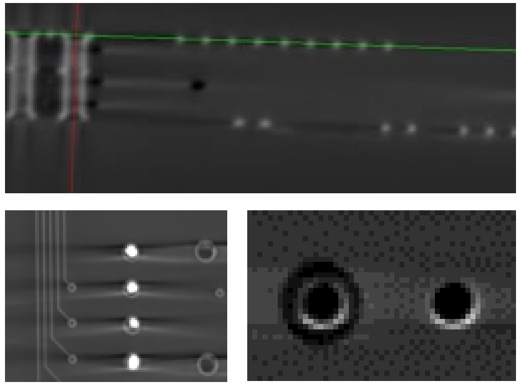
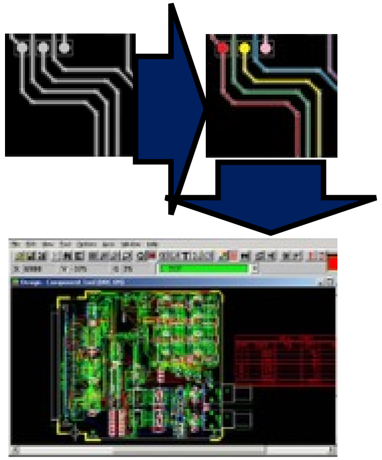


Image Processing and Segmentation

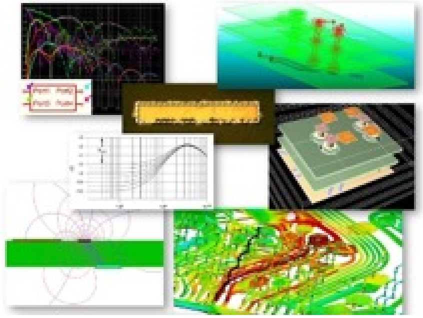
- Separate Layers
- Traces
- Vias w/ Pads
- Vias w/ Anti-Pads
- Conductive Planes

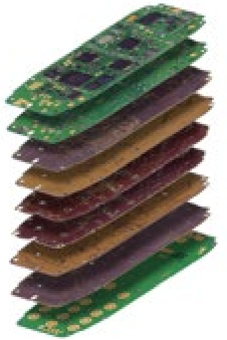
CAD File Generation

- Vectorization
- PCB CAD File (PCB, DWG, DXF, etc..)



Nondestructive!

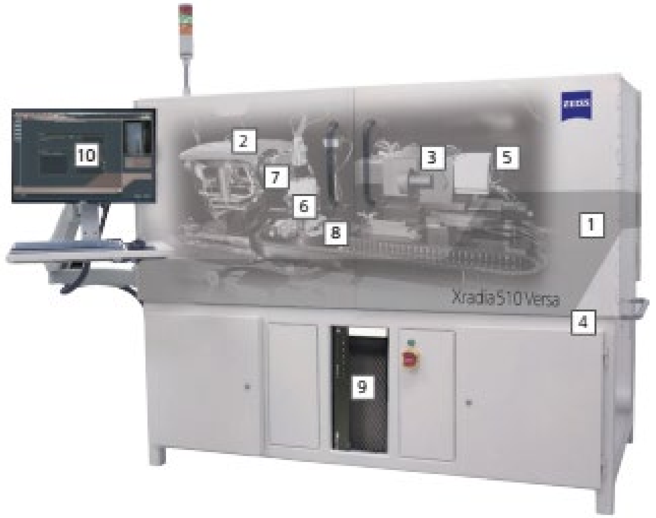


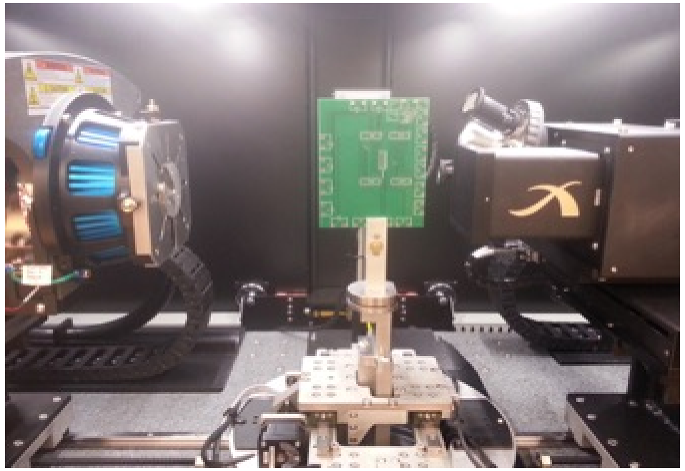


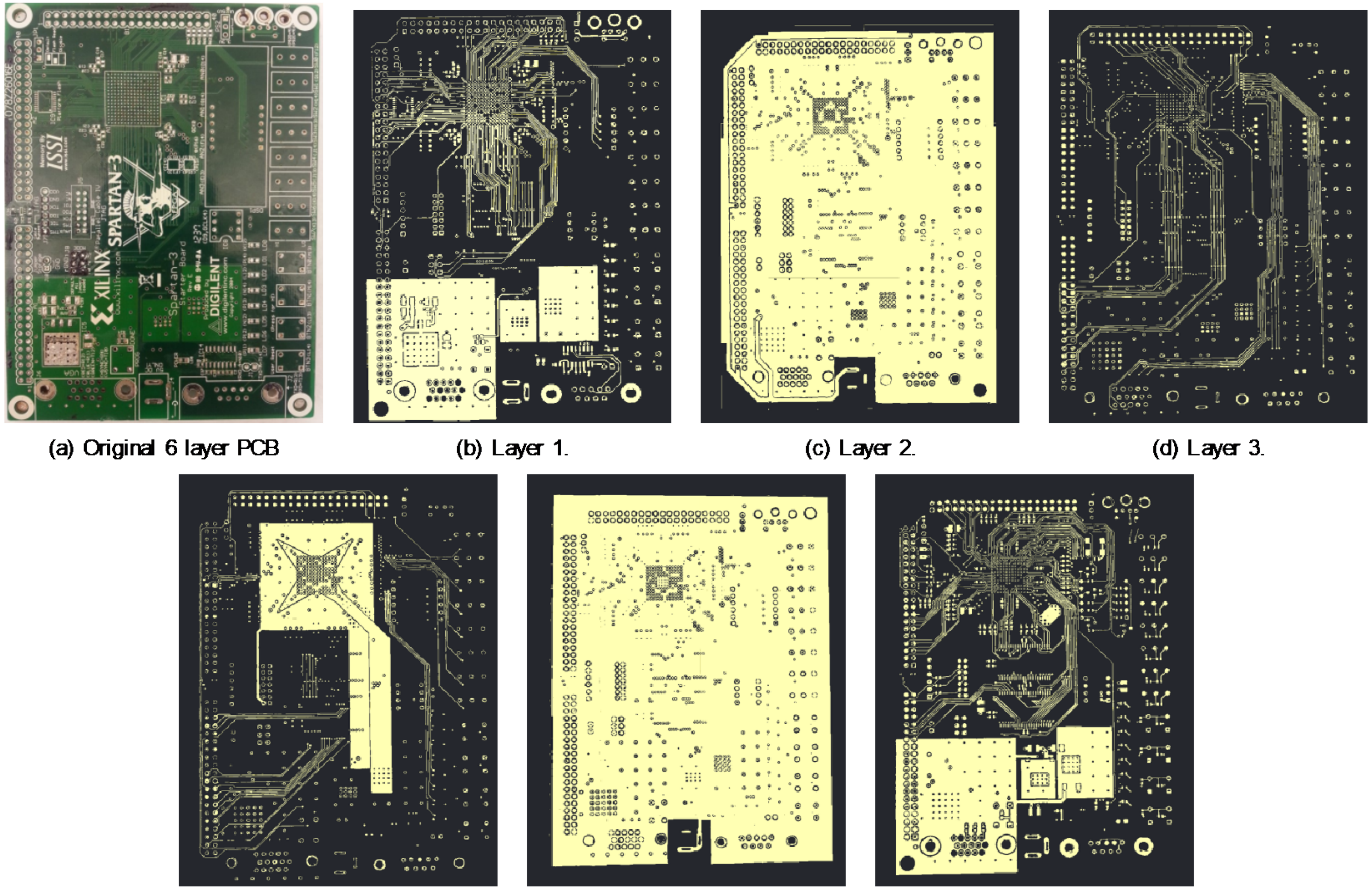
PCB Analysis

- Trace timing
- Signal integrity
- Power integrity
- Electromagnetic Interference
- Thermal Footprint
- Security vulnerabilities

Non-destructive Reverse Engineering







(a) Original 6 layer PCB

(b) Layer 1.

(c) Layer 2.

(d) Layer 3.

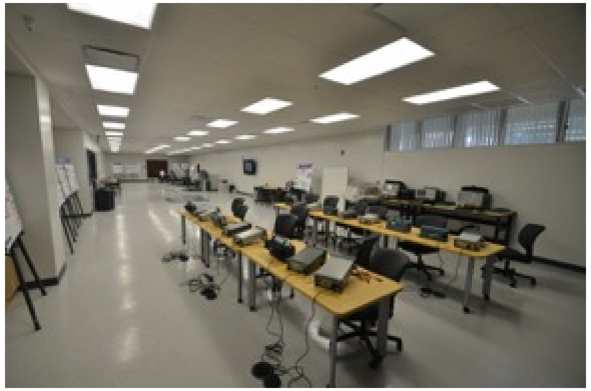
(e) Layer 4.

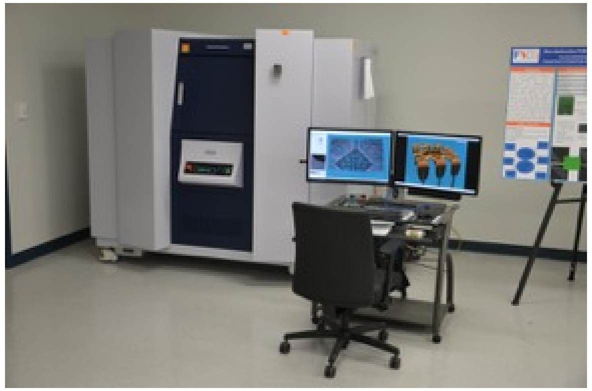
(f) Layer 5.

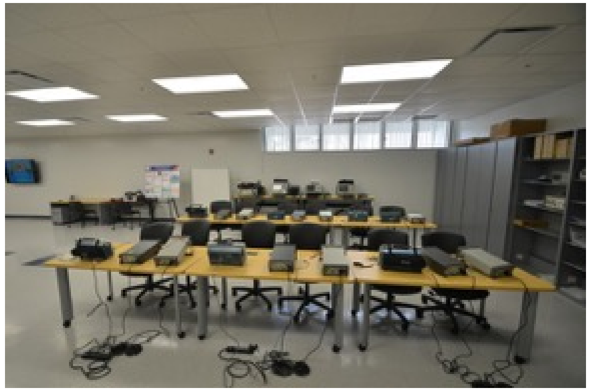
(g) Layer 6.

SCAN Lab at FICS Research Institute

Florida Institute for Cybersecurity (FICS) Research

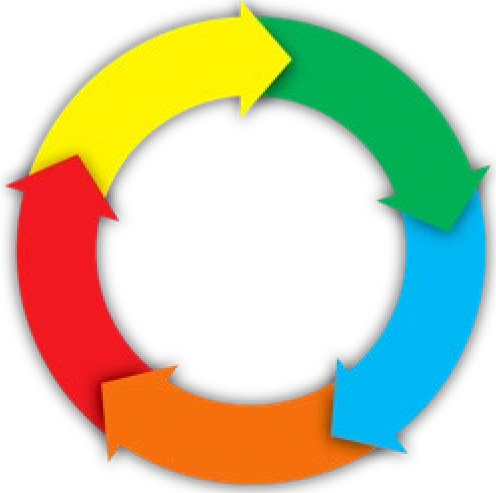






Recommendations

- **Designed-in security**
  - Standards: Logic Locking, SCA, Backside, Provenance, Traceability
- **Automation**
  - Reduce complexity & cost
- **Design with life cycle in mind**
  - Device → Systems
  - Traceability & provenance

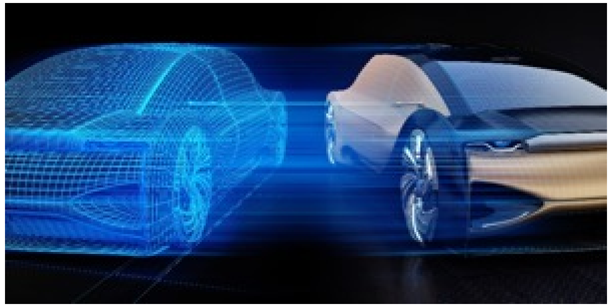


Recommendations

- **Powerful but low cost inspection**

- **Hardware upgrade → Zero day**

- **Smart devices → DT for secure semiconductors**



?