Securing Hardware for Designing Trustworthy Systems

Prabhat Mishra

Professor

Computer and Information Science and Engineering

University of Florida, USA

UF UNIVERSITY of FLORIDA | EMBEDDED SYSTEMS LAB

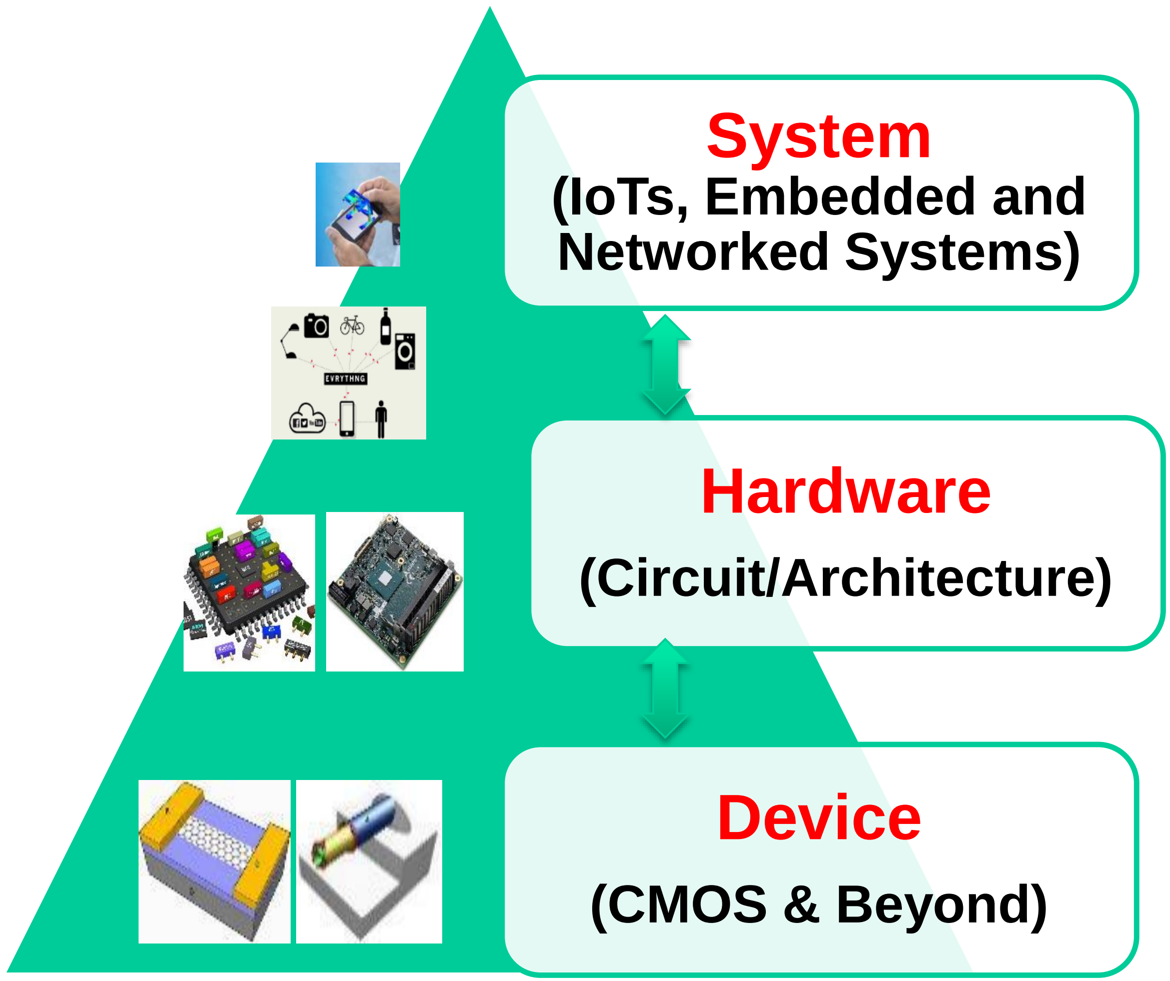
Outline

- Introduction
- Design for Security
- Security Attacks and Countermeasures
- Security and Trust Validation
- Application-Specific Security
- Conclusion

Outline

- Introduction
  - Introduction to Hardware Security Vulnerabilities
  - System-on-Chip Design using Potentially Untrusted Third-Party IPs
- Design for Security
- Security Attacks and Countermeasures
- Security and Trust Validation
- Application-Specific Security
- Conclusion

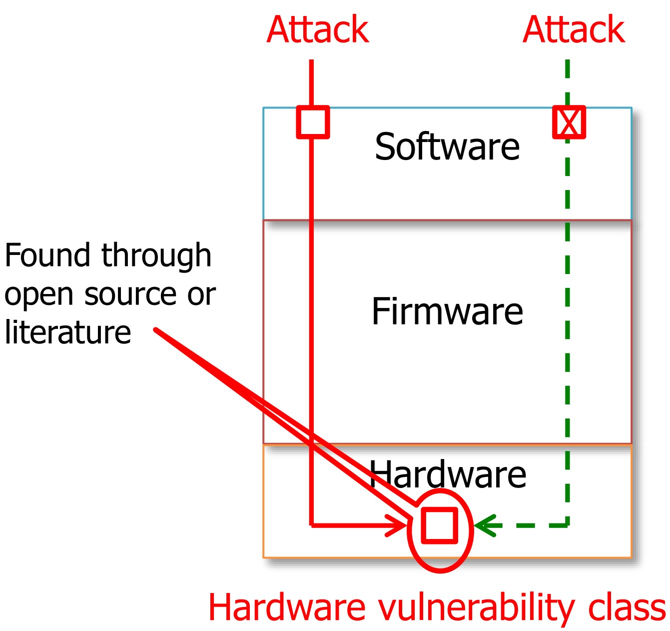
Secure Connected Systems



Why Hardware Security?

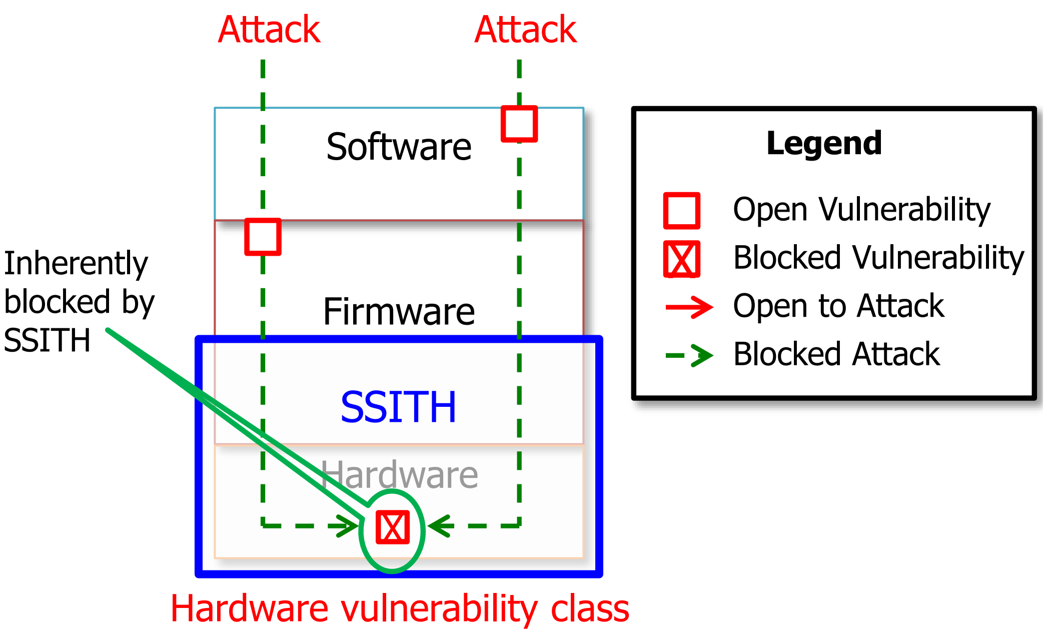
Today: Patch and Pray

*2800 vulnerability instances
2800 software patches



Future: SSITH

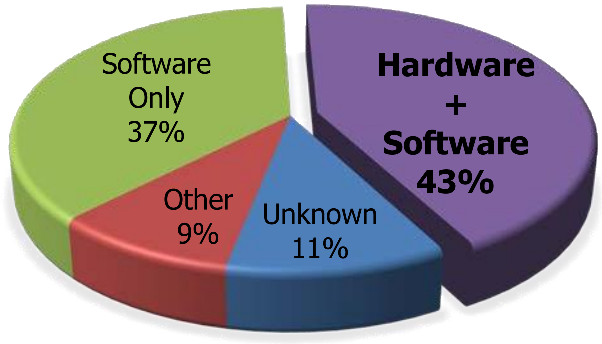
SSITH will protect against all 7 hardware classes



*7 vulnerability classes
7 hardware solutions

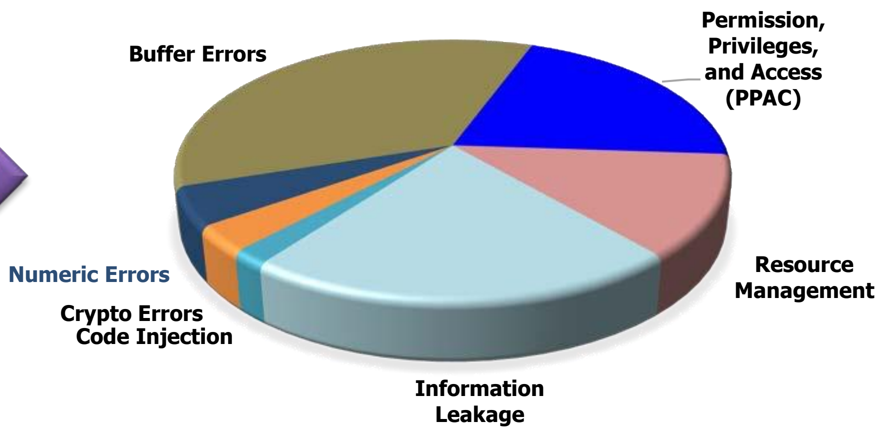
Scope of Hardware Security

Electronic System Vulnerabilities

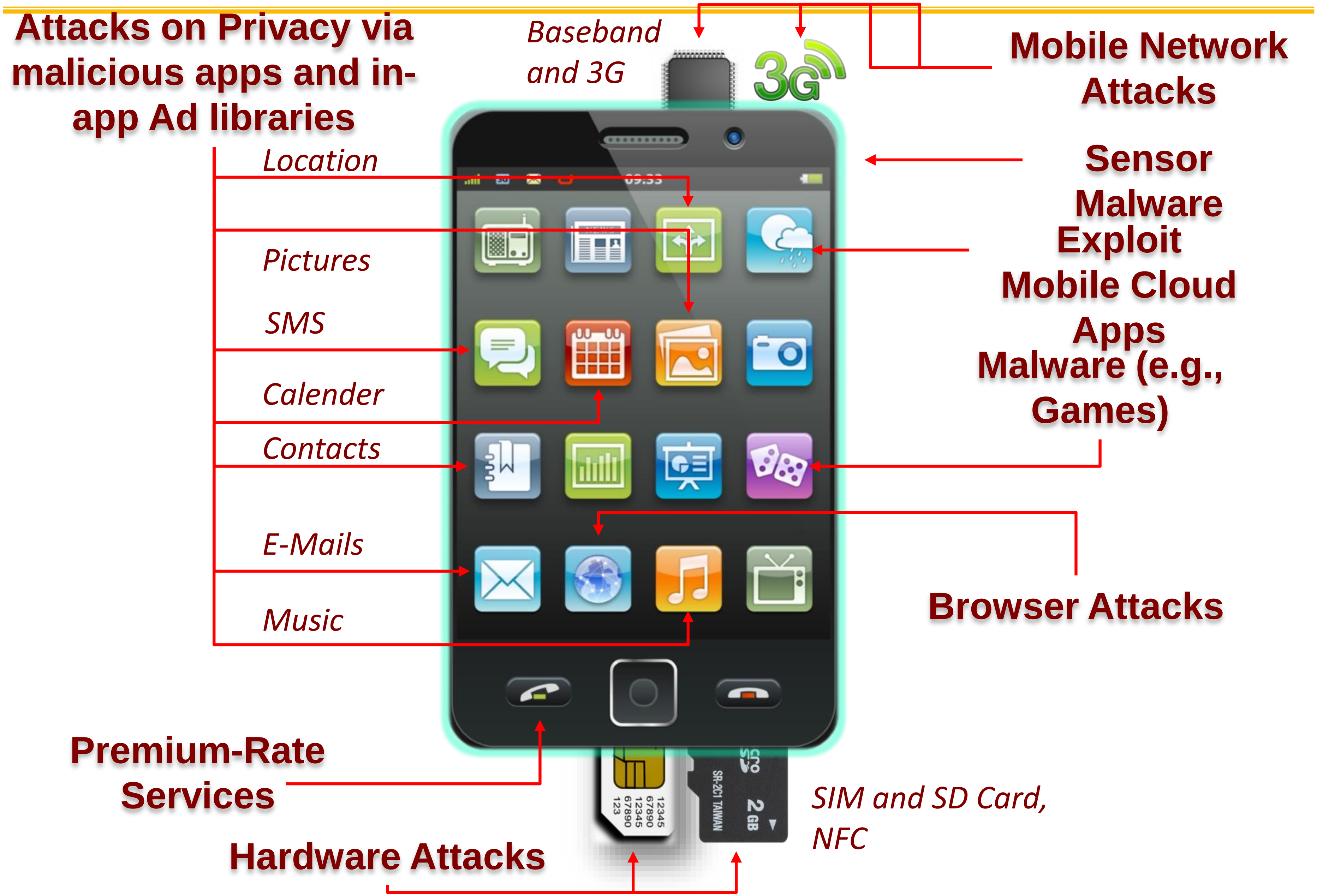


Data from MITRE/NIST CVE website

Hardware+ Software Vulnerabilities



Mobile Devices: Attack Surface

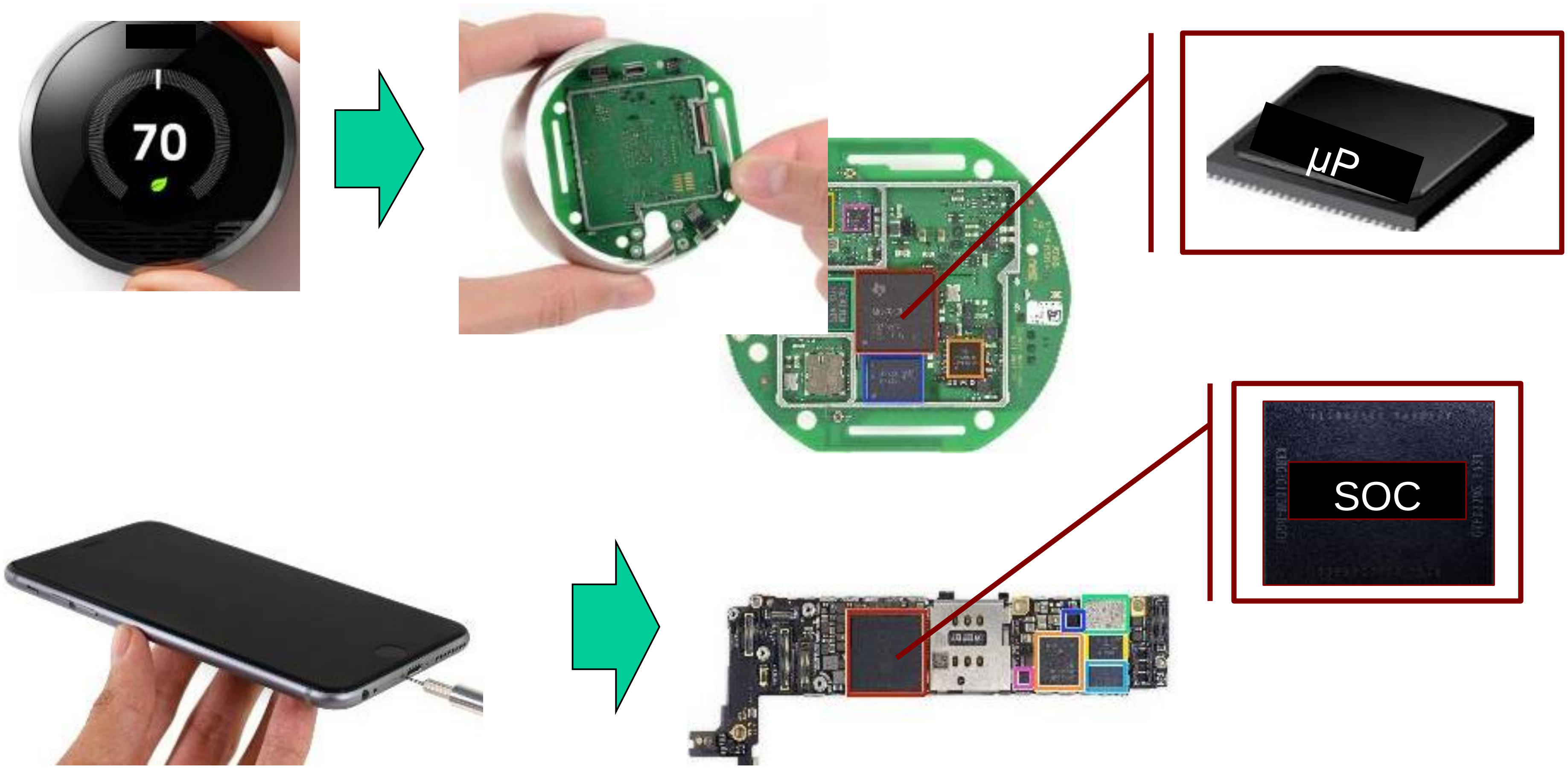


Example Attacks

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

What is Hardware?

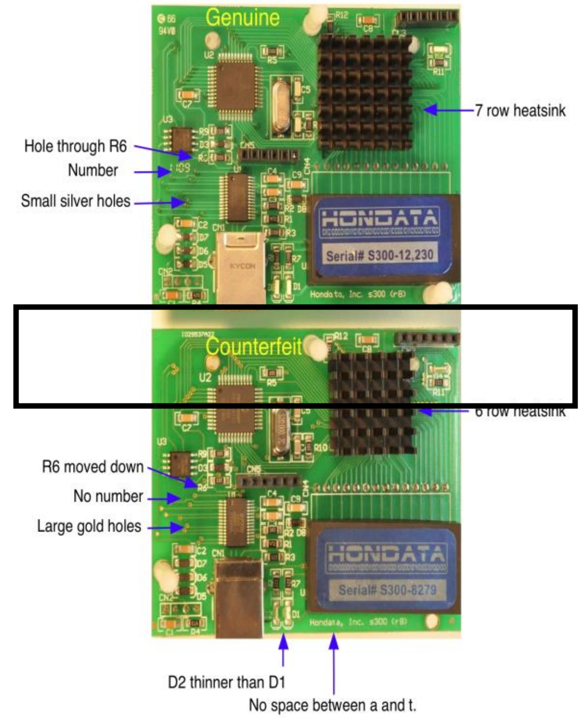


- Electronic System
- System Hardware – acts as the ***"root-of-trust"***: PCB → IC (SoC | µP)

Motivation – HW Security

- **HW security is a serious concern**
  - Hardware security sneaks into PCs, Robert Lemos, *CNET News.com, 3/16/05*
  - Microsoft reveals hardware security plans, concerns remain, *Robert Lemos, SecurityFocus 04/26/05*
  - Princeton Professor Finds No Hardware Security In E-Voting Machine, A. Gonsalves, InformationWeek 02/16/07
  - Secure Chips for Gadgets Set to Soar, *John P. Mello Jr. TechNewsWorld, 05/16/07*
  - Army requires security hardware for all PCs, *Cheryl Gerber, FCW.com, 7/31/2006*
  - Visit Facebook group on Hardware Security

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

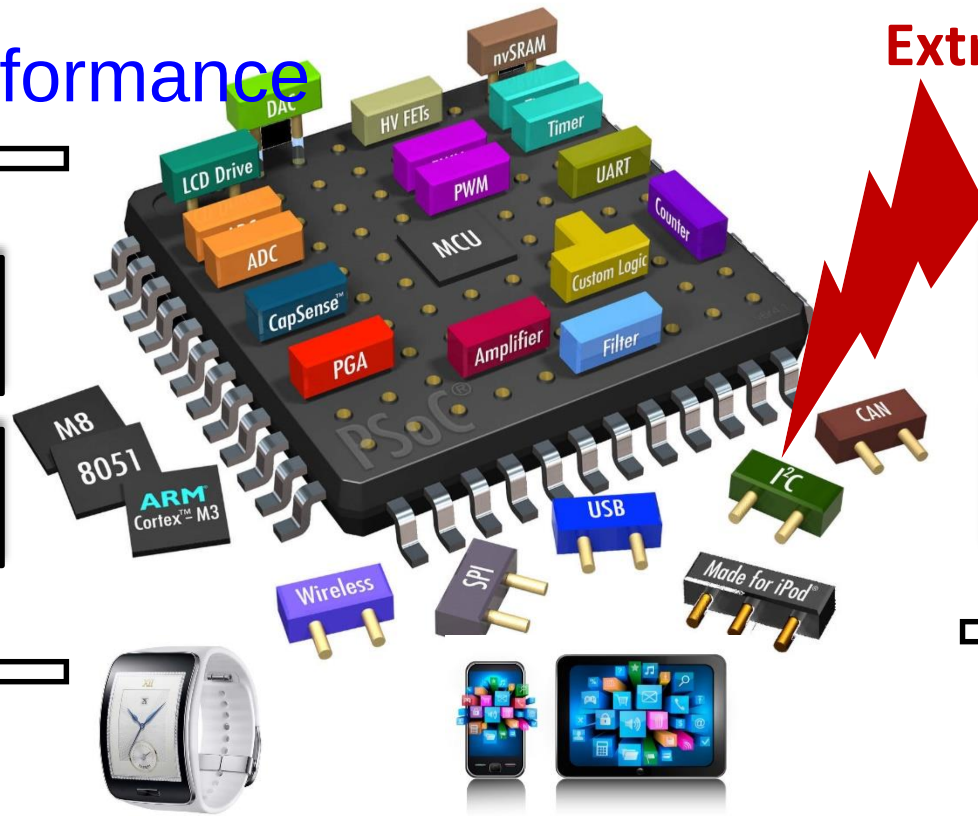
Outline

- Introduction
  - Introduction to Hardware Security Vulnerabilities
  - System-on-Chip Design using Potentially Untrusted Third-Party IPs
- Design for Security
- Security Attacks and Countermeasures
- Security and Trust Validation
- Application-Specific Security
- Conclusion

System on Chips (SoC)

- All electronic system components
  - One single chip (SoC)
  - Multiple Intellectual Property (IP) blocks
  - Cost effective
  - Better Performance

Ensuring Security is Extremely Difficult



Integration of Third-Party IPs

Untrusted Supply Chain

Huge Complexity

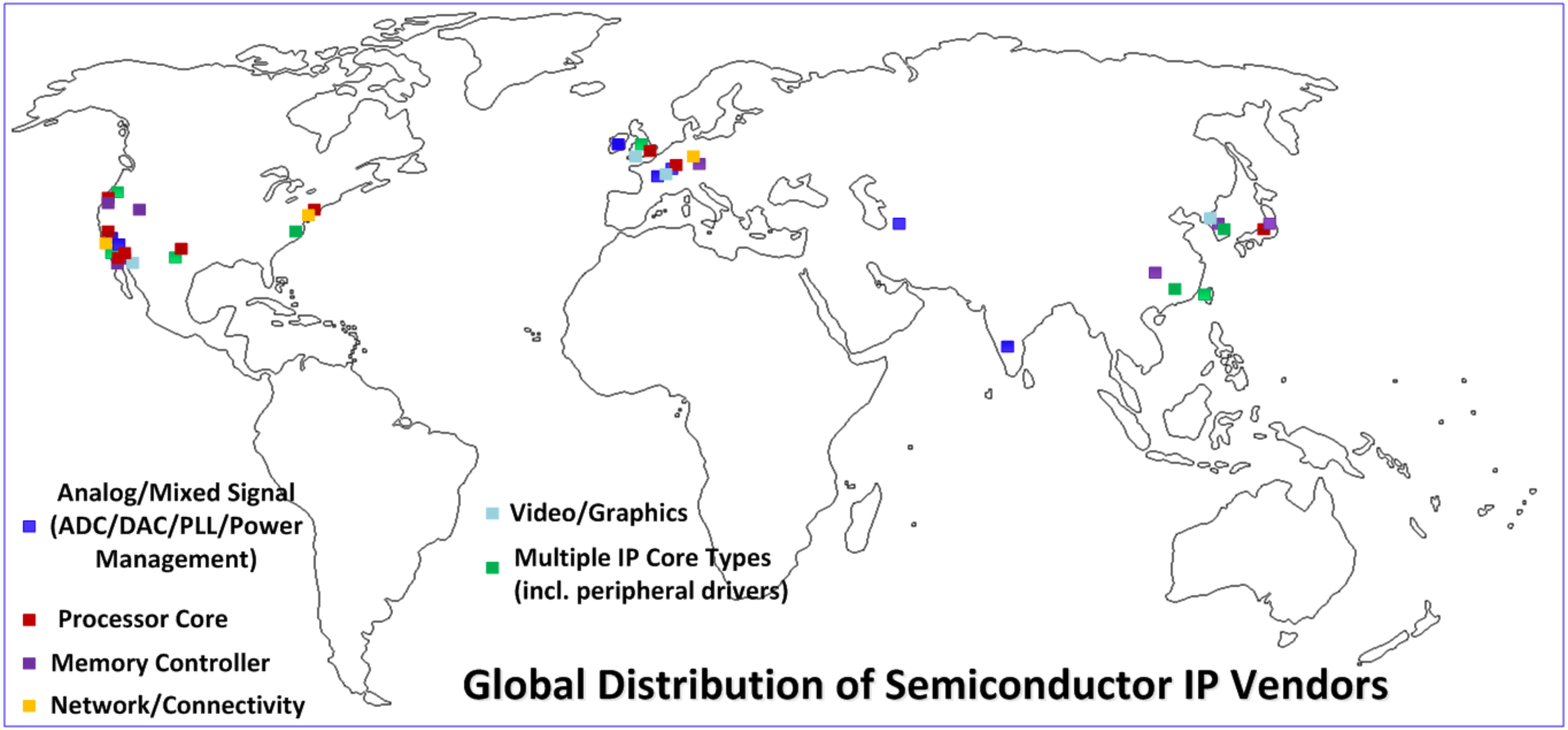
Many Custom Functionality

Some Basic Definitions

- **Intellectual property** represents the property of your mind or intellect - proprietary knowledge

- The four legally defined forms of IP
  - **Patents** When you register your invention with the government, you gain the legal right to exclude anyone else from manufacturing or marketing it
  - **Trademarks** A trademark is a name, phrase, sound or symbol used in association with services or products
  - **Copyrights** Copyright laws protect written or artistic expressions fixed in a tangible medium
  - **Trade secrets** A formula, pattern, device or compilation of data that grants the user an advantage over competitors

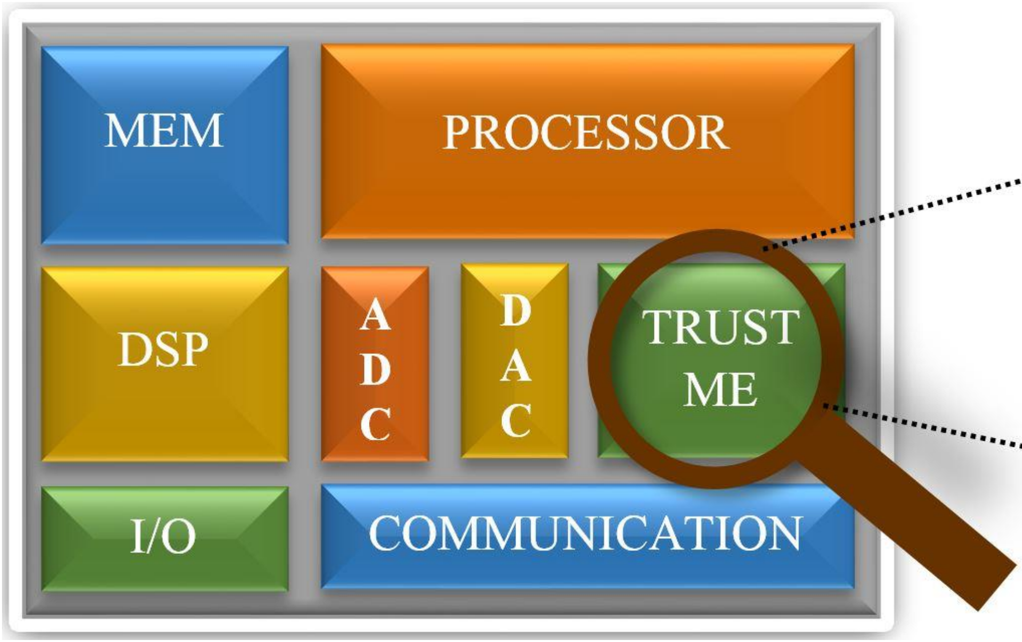
SoC Design using Intellectual Property (IP) Blocks



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

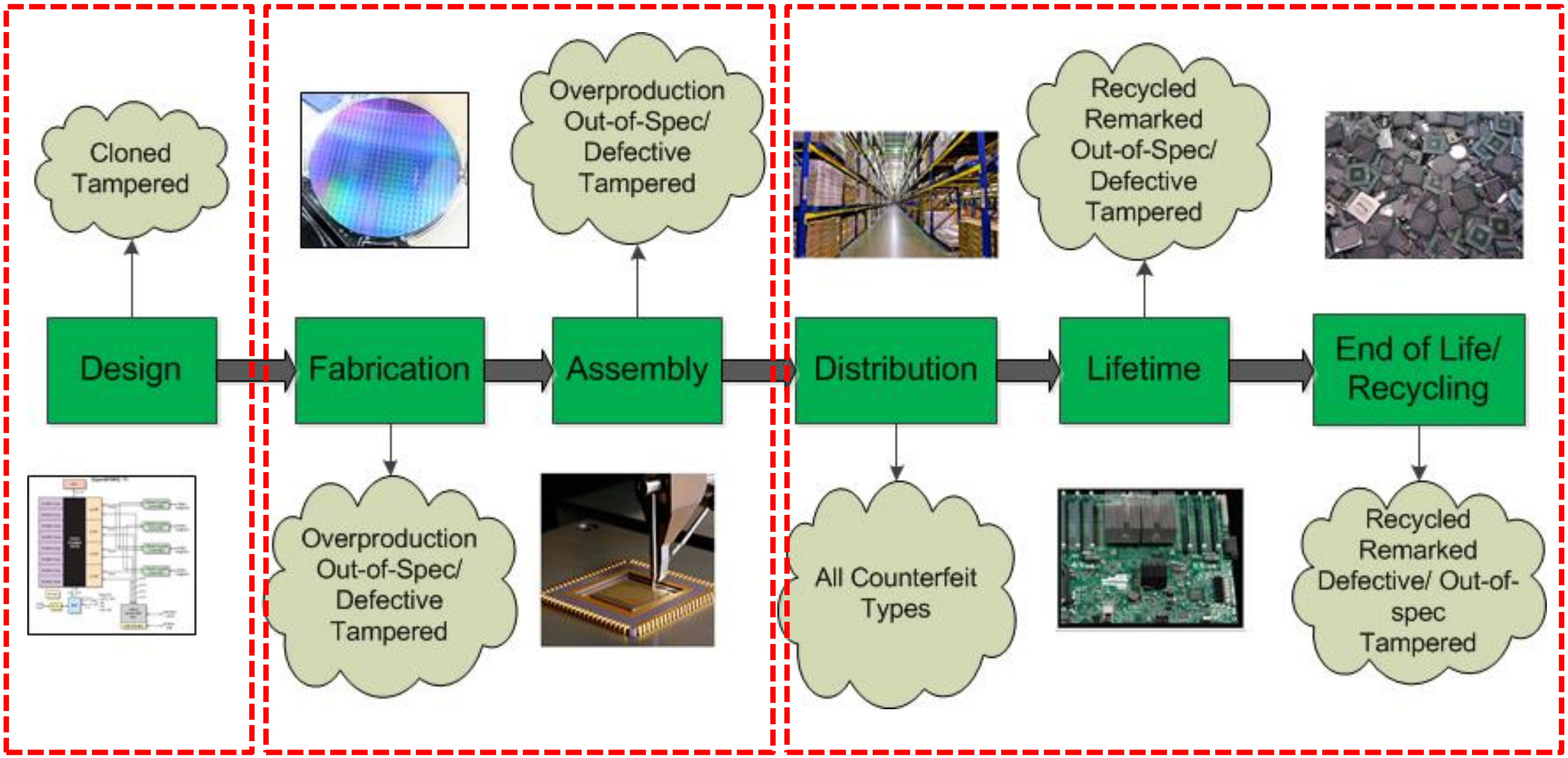
P. Mishra, S. Bhunia and M. Tehranipoor, Hardware IP Security and Trust, Springer, 2017.

Trust Me!



F. Farahmandi, Y. Huang and P. Mishra, System-on-Chip Security Validation and Verification, Springer, ISBN: 978-3-030-30596-3, 2019.

Electronics Supply Chain Security



Untrusted IP Vendor & Sys. Integrator

Untrusted Foundry & Assembly

In the Field & Recycling

Maximum Flexibility

Minimum Flexibility

Outline

- Introduction
- Design for Security
  - Cryptography and Random Number Generator
  - Logic Locking and Obfuscation
  - Watermarking and Physical Unclonable Functions
- Security Attacks and Countermeasures
- Security and Trust Validation
- Application-Specific Security
- Conclusion

What We Want to Achieve?

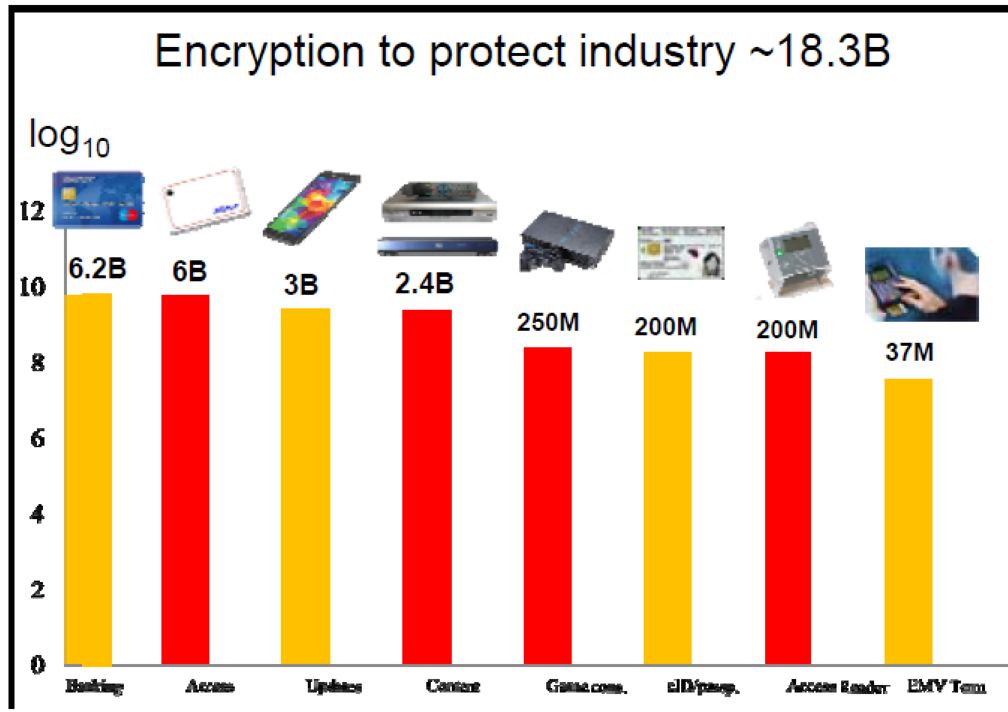
Authentication
no spoofing

Data Integrity
no data alteration

Privacy
no eavesdropping

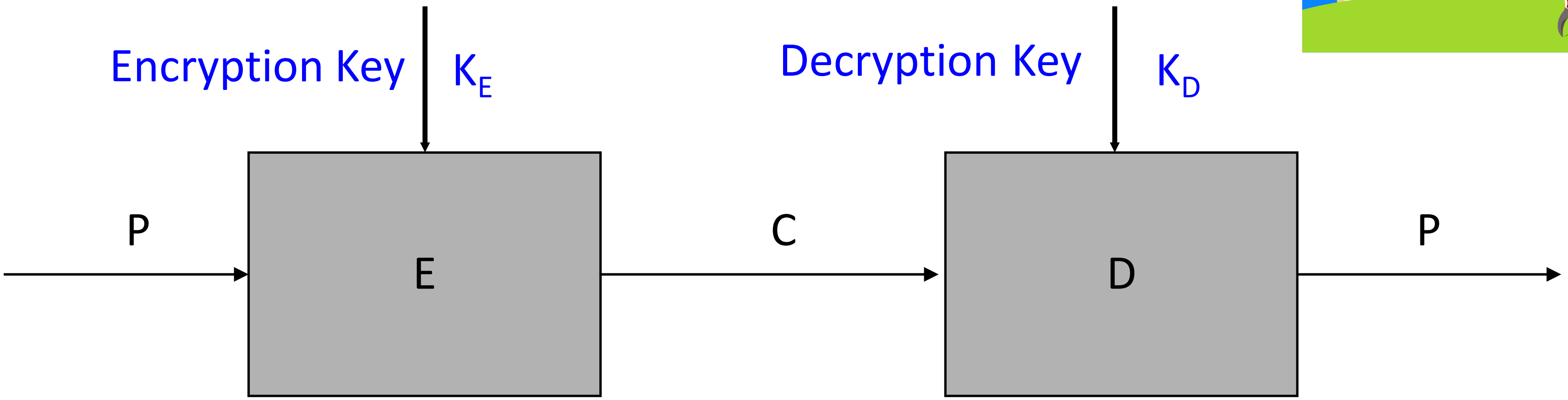
Cryptography Plays an Important Role

- Crypto principles see growing usage in information protection
- A locking approach



Cryptographic algorithms protects critical infrastructure and assets!

Crypto System with Keys



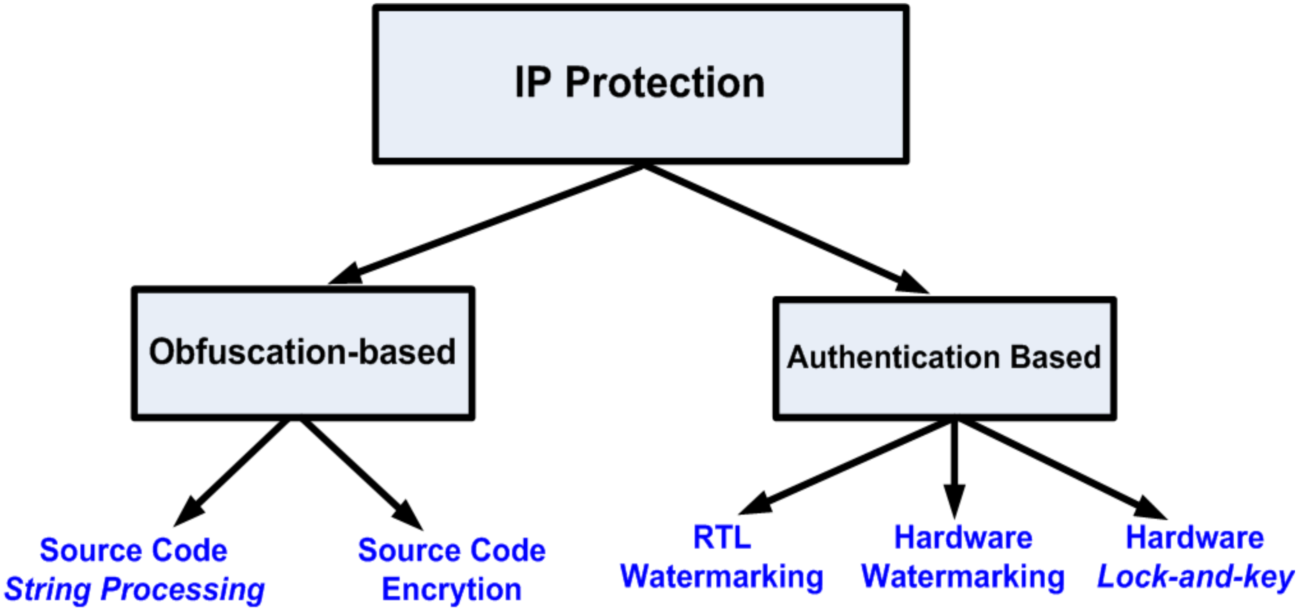
- $C = E(K_E, P)$
  - E = *set* of encryption algorithms / K_E selects $E_i \in E$
- $P = D(K_D, C)$
  - D = *set* of decryption algorithms / K_D selects $D_j \in D$
- Crypto algorithms and keys are like door locks and keys
- We need: $P = D(K_D, E(K_E, P))$

Classification of Cryptosystems w.r.t. Keys

- Keyless cryptosystems exist (e.g., Caesar's cipher)
  - Less secure
- Symmetric cryptosystems: $K_E = K_D$
  - Classic
  - Encipher and decipher using the same key
    - Or one key is easily derived from other
- Asymmetric cryptosystems: $K_E \neq K_D$
  - Public key system
  - Encipher and decipher using different keys
    - Computationally infeasible to derive one from other

Hardware Obfuscation for IP Protection

- Global Hardware Piracy estimated at $1B/day*
- Causes loss of market share, revenue and reputation
- Affects all parties (IP vendors, IC design houses and System Designers)



Watermark Example

```
case (case_select)
    3’d0 : out = 4’d1;
    3’d3 : out = 4’d4;
    3’d5:  out = 4’d6;
    3’d7:  out = 4’d8;
    default : out =
    4’b0;
endcase
```

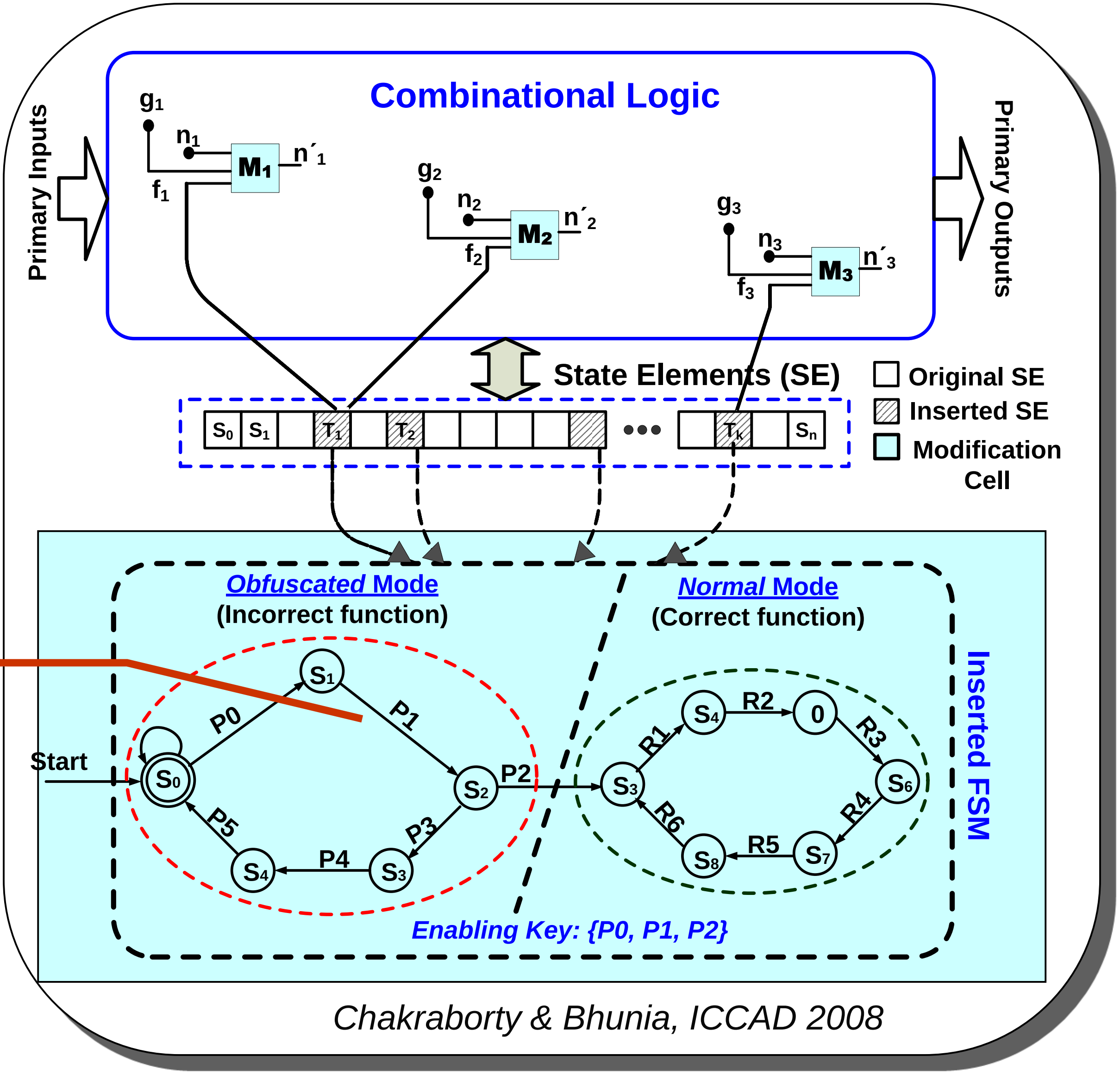
Castillo *et al*, *TVLSI*, 2007

**http://vsi.org/documents/datasheets/TOCIPPWP210.pdf*

Security through Key-based Obfuscation

Basic Idea:

- Obfuscate the design functionally and structurally
- Achieved by modifying the state transition function
- Normal behavior is _enabled_ only upon application of a key!



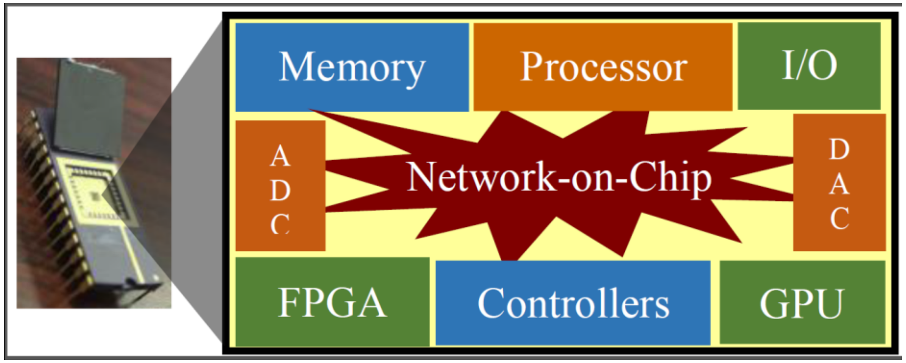
Chakraborty & Bhunia, ICCAD 2008

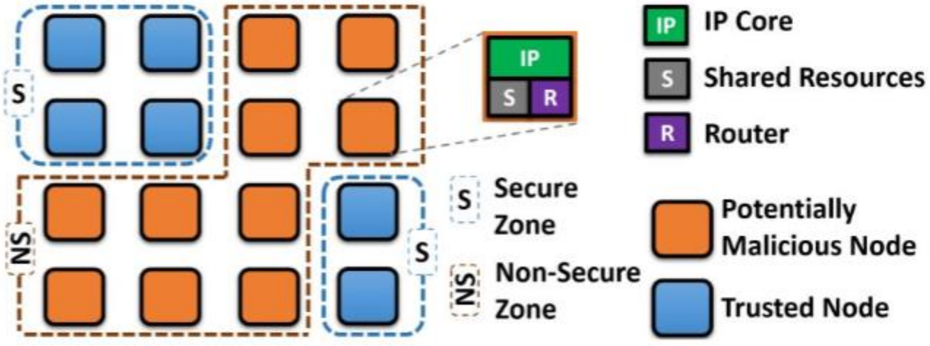
Prevents illegal usage of IPs!

Chakraborty & Bhunia, TCAD 2009

Design for Security

- IP Specific (Network-on-Chip) Protection
  - Anonymous Routing
  - Trust-aware Routing
  - Authenticated Encryption
  - Detection and Localization of DoS

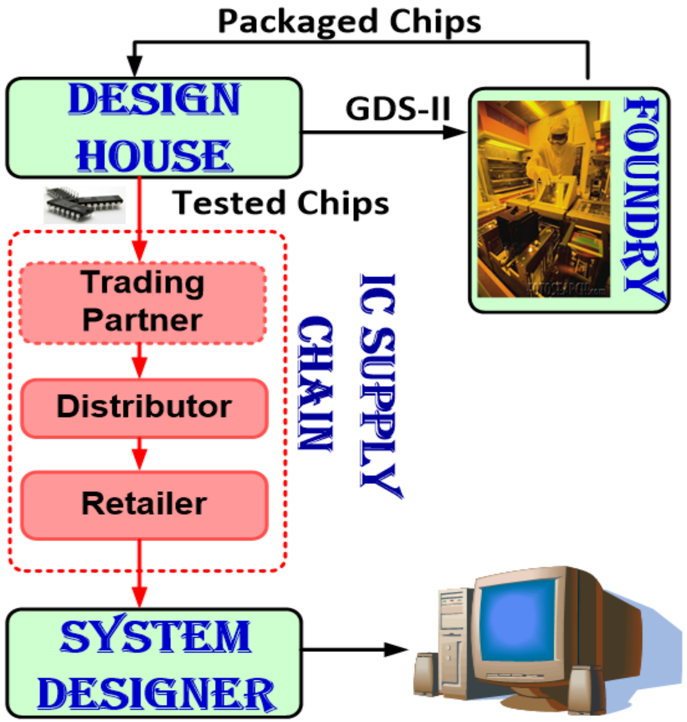




S. Charles, Y. Lyu, P. Mishra, Real-time Detection and Localization of DoS Attacks in NoC based SoCs, Design Automation and Test in Europe (DATE), Florence, Italy, 2019.

Counterfeit ICs: A Rising Concern

- Globally distributed semiconductor business model
  - Ample *sneak paths* to insert counterfeit chips

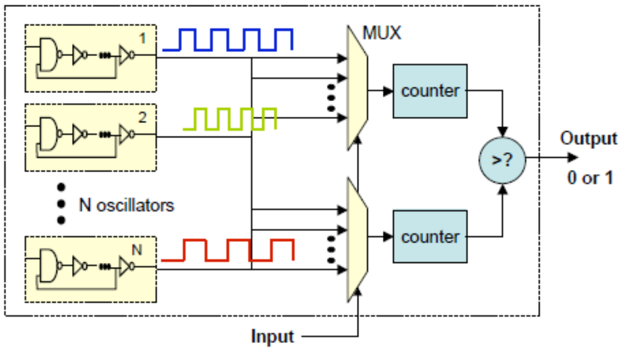


Q: How do we solve?

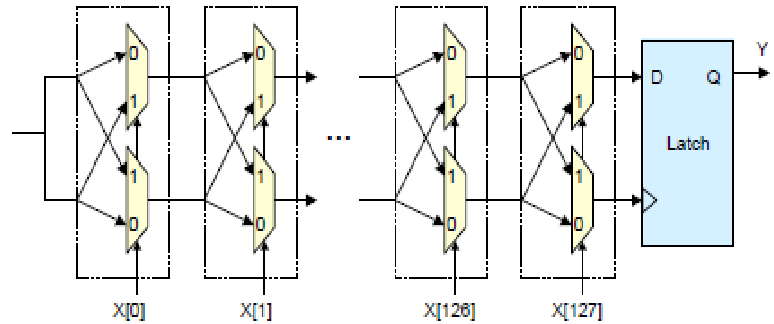
A: IC Fingerprinting

- Two Broad Categories:
  - ***Recycled/Remarked:*** selling of used/aged chips as new
  - ***Cloned Chips::*** IP piracy, reverse-engineering., overproduction

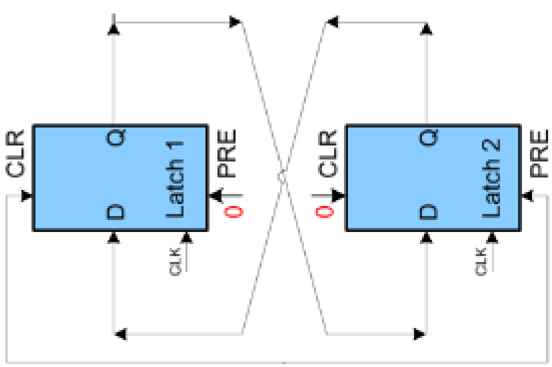
Physical Unclonable Functions (PUFs)



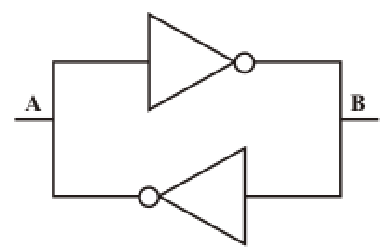
RO PUF
-Gassend *et al, 2002,* Suh *et al, 2007*



Arbiter PUF
-Lee *et al, 2004*



Butterfly PUF
-Kumar *et al,* 2008



PUF using on-chip structure!

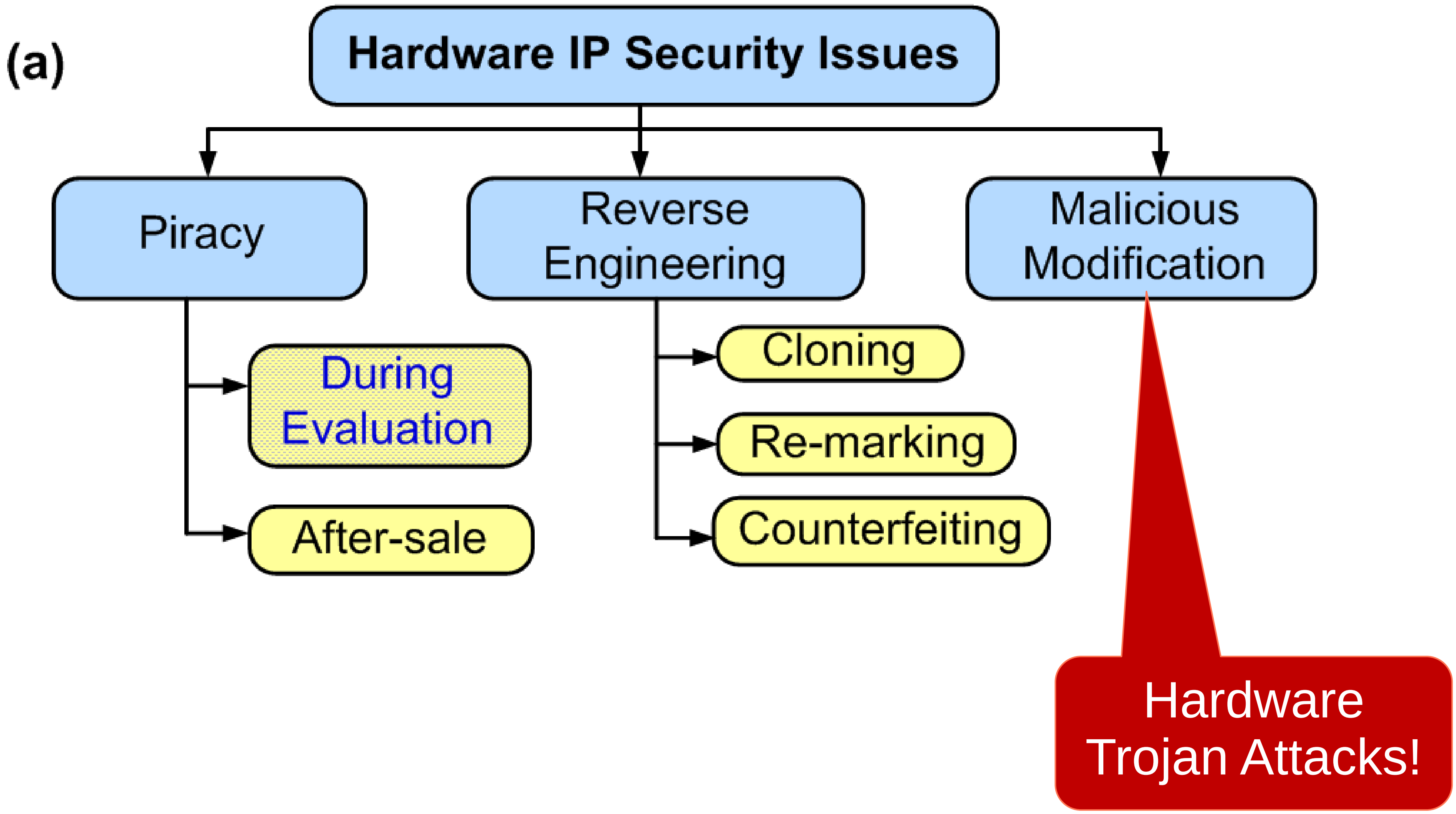
SRAM PUF
-Guajardo *et al,* Holcomb *et al,* 2007

Generate "robust" "strong" PUF using on-chip structure

Outline

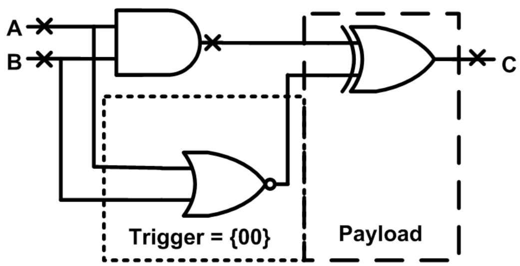
- Introduction
- Design for Security
- Security Attacks and Countermeasures
  - Hardware Trojans
  - Side Channel Attacks
  - Exploitation of Test and Debug Structures
- Security and Trust Validation
- Application-Specific Security
- Conclusion

What are the Challenges?

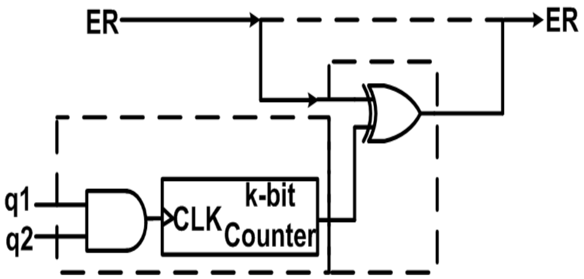


HW Trojan Examples/Models

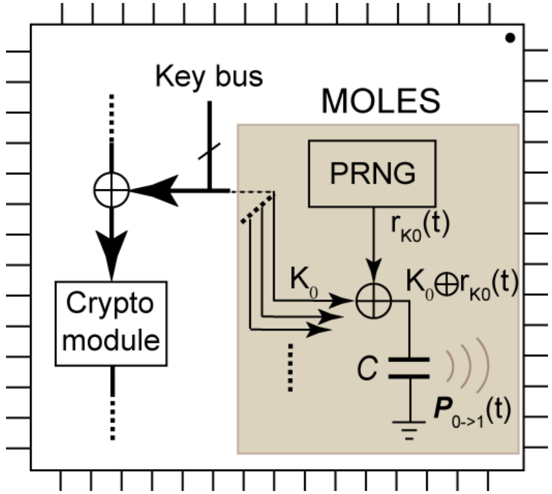
Comb Trojan Example



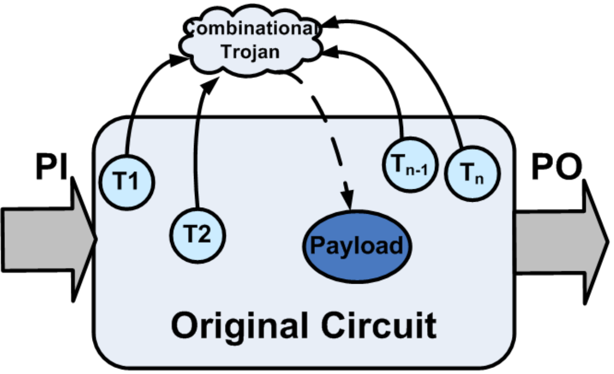
Seq Trojan Example



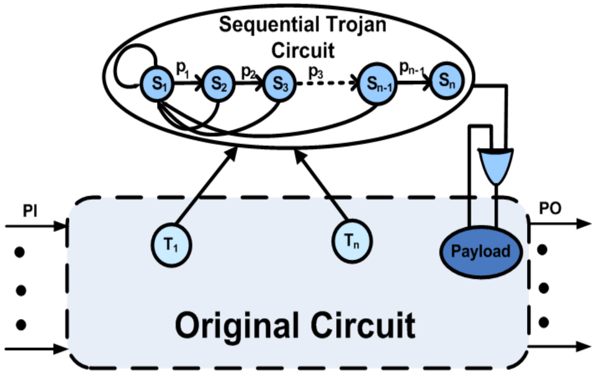
MOLES*: Info Leakage Trojan

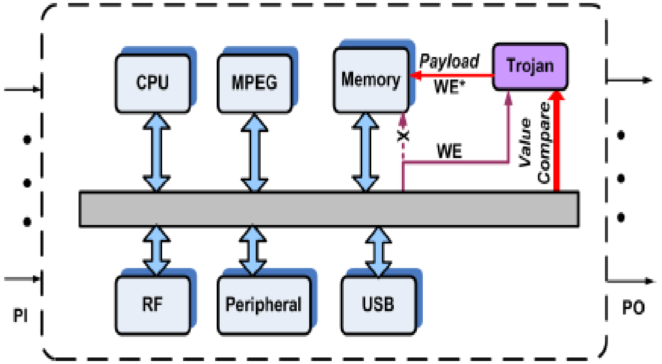


Comb Trojan model



Seq. Trojan Model

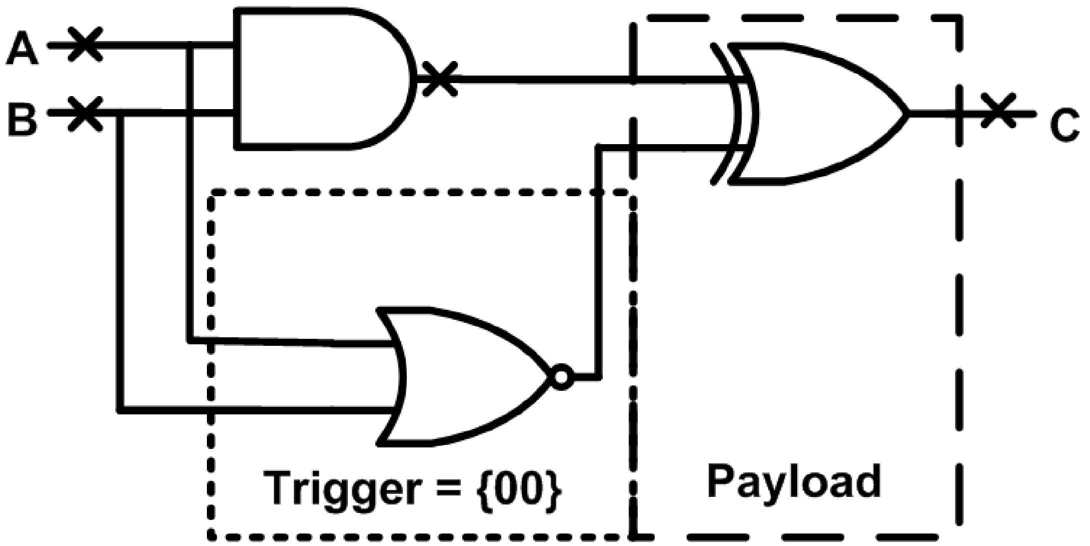




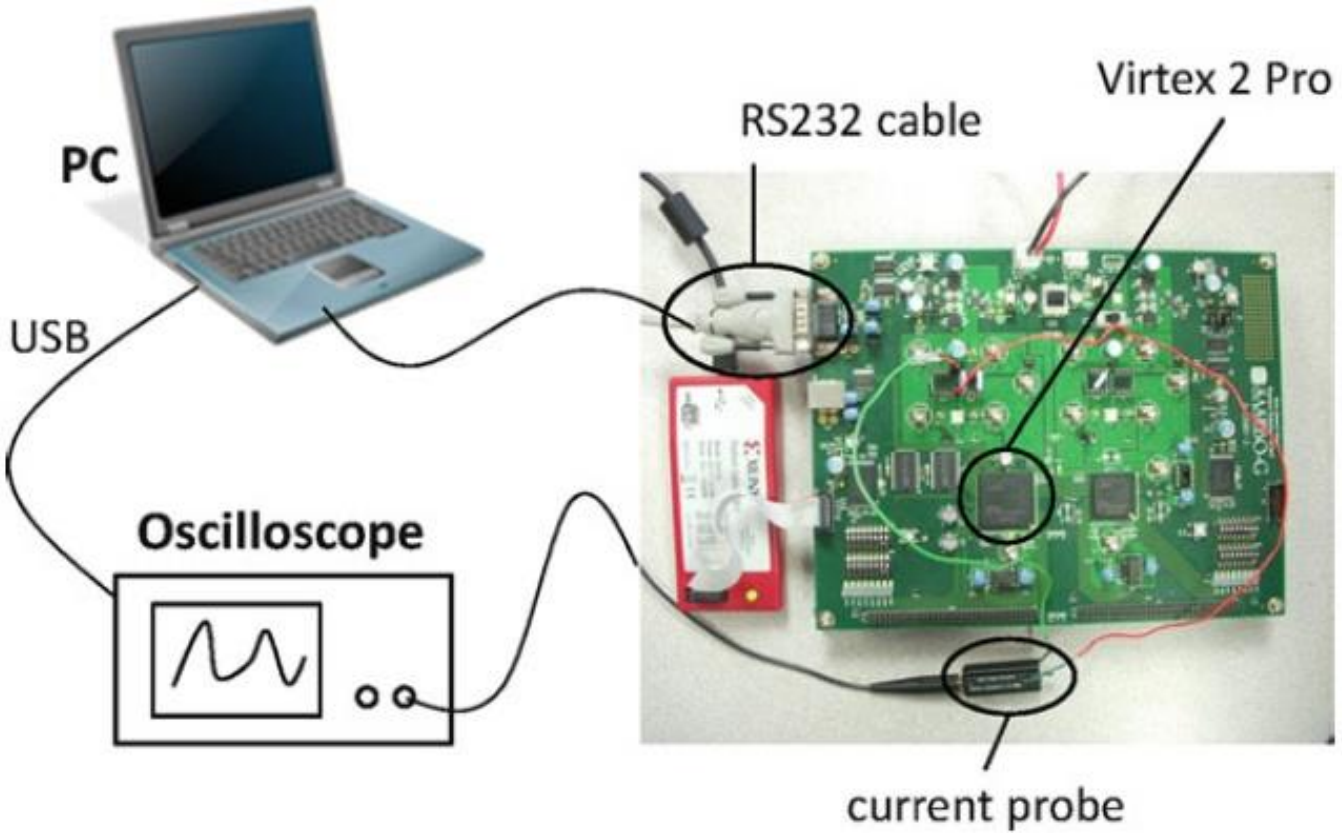
System level view

Why is Trojan Detection Challenging?

- Trojans are stealthy
  - Conventional ATPG is not effective
- Inordinately large number of possible Trojan instances
  - Combinatorial dependence on number of circuit nodes
  - 8-bit ALU (*c880*) with 451 nodes → ~10^{11} possible 4-input Trojans!
- Sequential Trojans extremely hard to detect

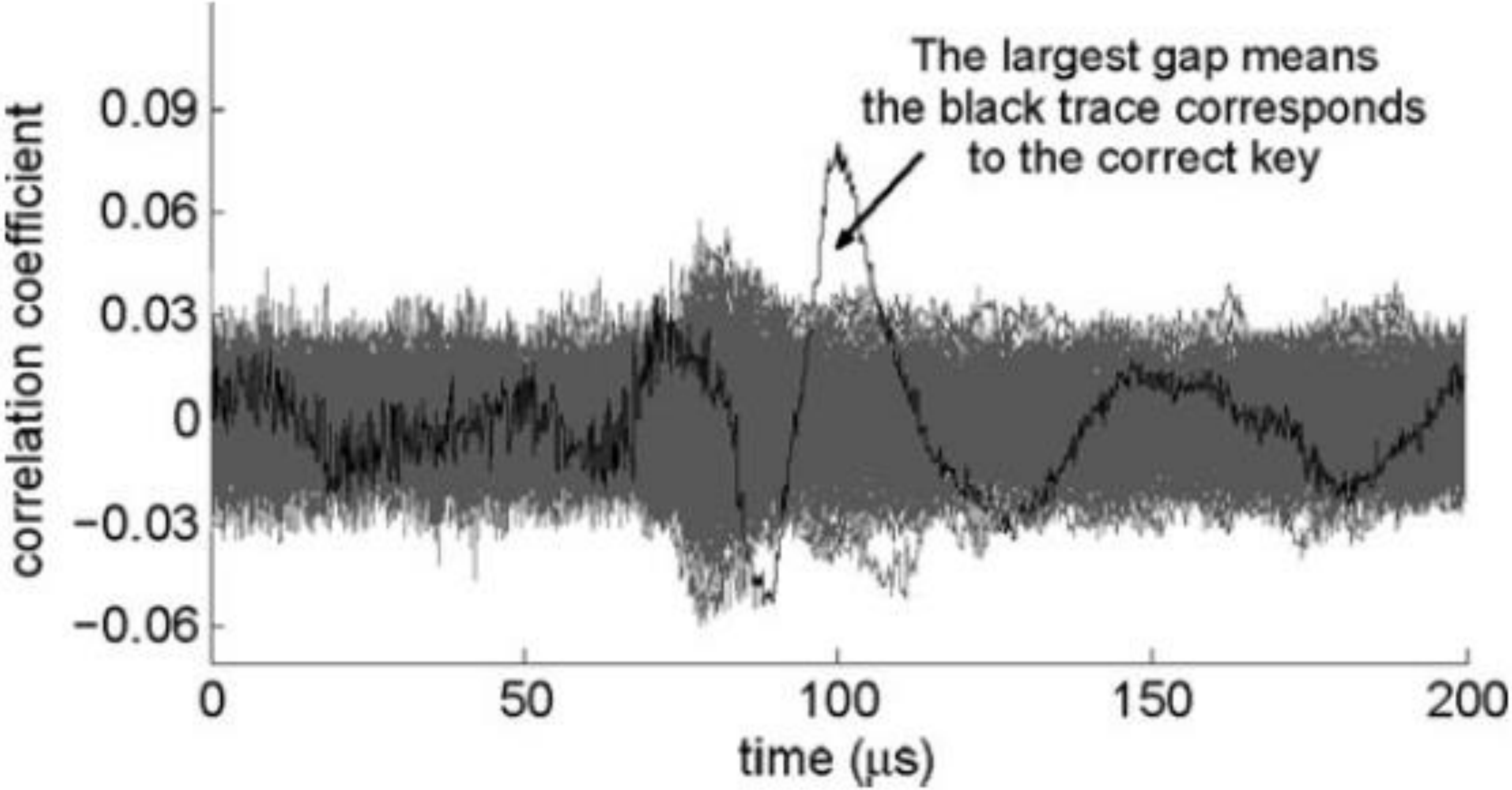


Side-Channel Attacks on Microcontrollers



- The PC sends a sample plaintext to the PowerPC on the FPGA for encryption. During the encryption, the digital oscilloscope captures the power consumption from the board. After the encryption is completed, the PC downloads the resulting power trace from the oscilloscope, and proceeds with the next sample plaintext.

Practical Hypothesis Tests



- An example of 256 correlation coefficient traces. Around time 100 us, the black trace which corresponds to the correct key byte emerges from all the other 255 traces.

Side-Channel Leakage

Physical attacks ≠ Cryptanalysis

(gray box, physics) (black box, maths)

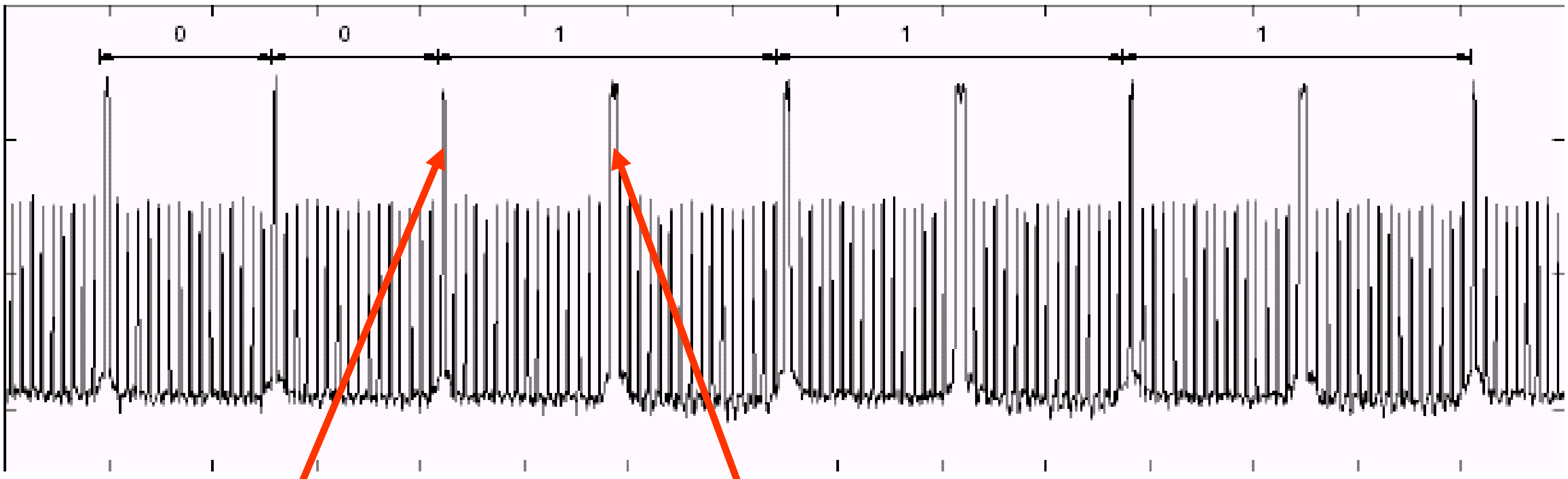
- Does not tackle the algorithm's math

- Observe physical quantities in the device's vincinity and use additional information during cryptanalysis

Power Analysis Attack

Idea: During switching CMOS gates draw spiked current

Trace of Current drawn - RSA Secret Key Computation



Only Squaring

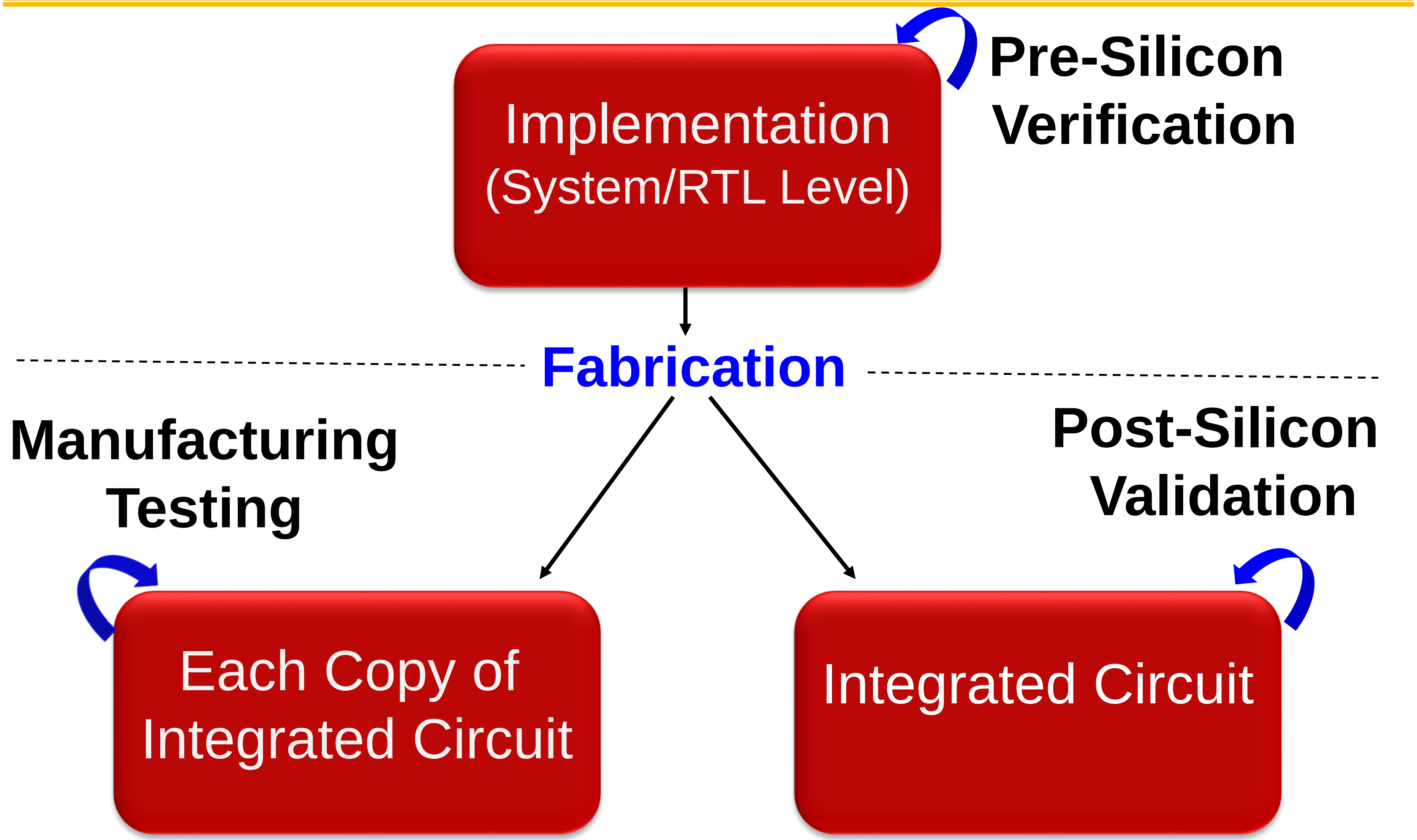
Squaring and multiplication

Reported Results : Every Smartcard in the market BROKEN

Outline

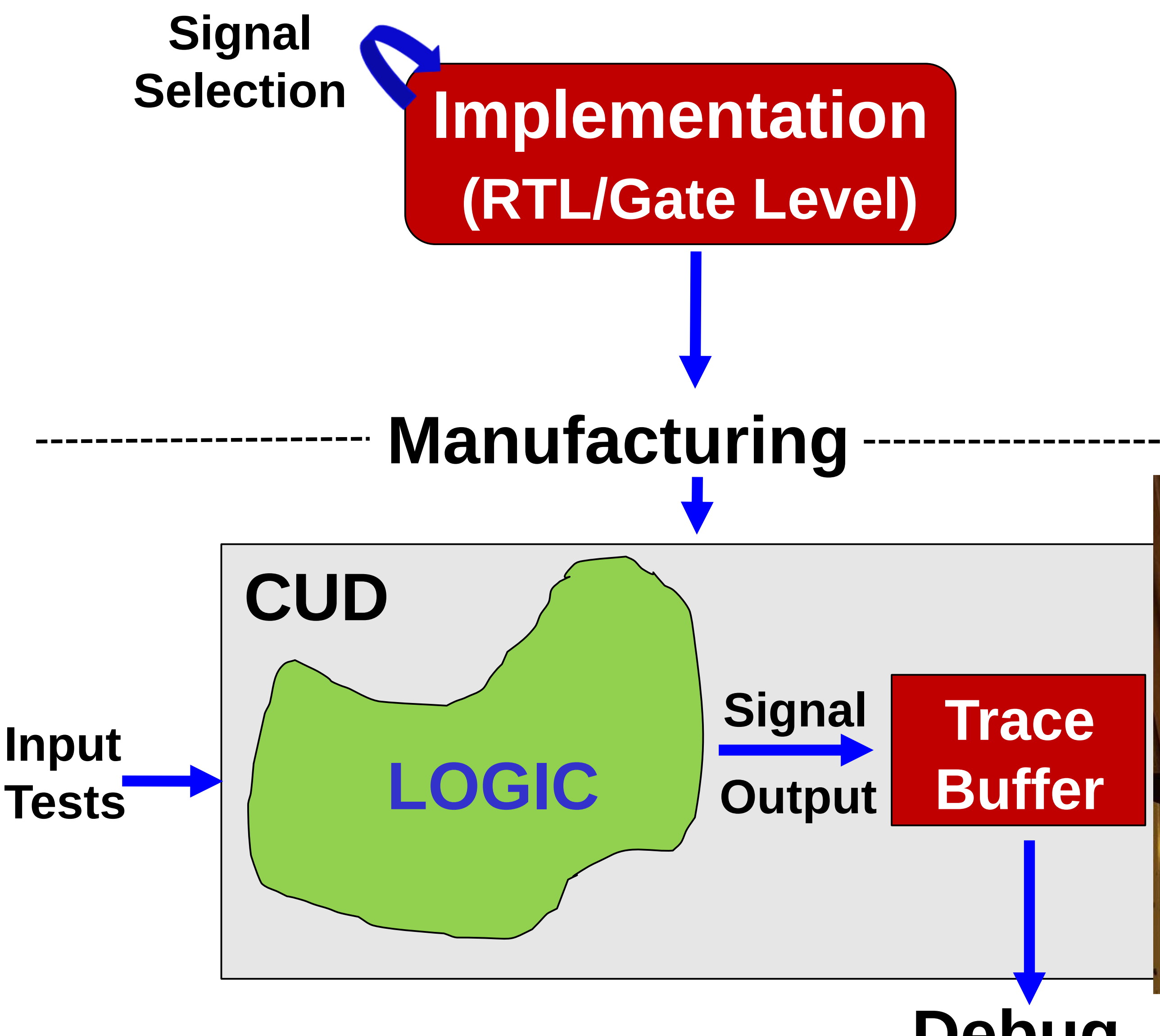
- Introduction
- Design for Security
- Security Attacks and Countermeasures
- Security and Trust Validation
  - Simulation-based Security Validation
  - Security Validation using Side Channel Analysis
  - IP Trust Validation using Formal Methods
- Application-Specific Security
- Conclusion

Validation of System-on-Chip (SoC) Designs



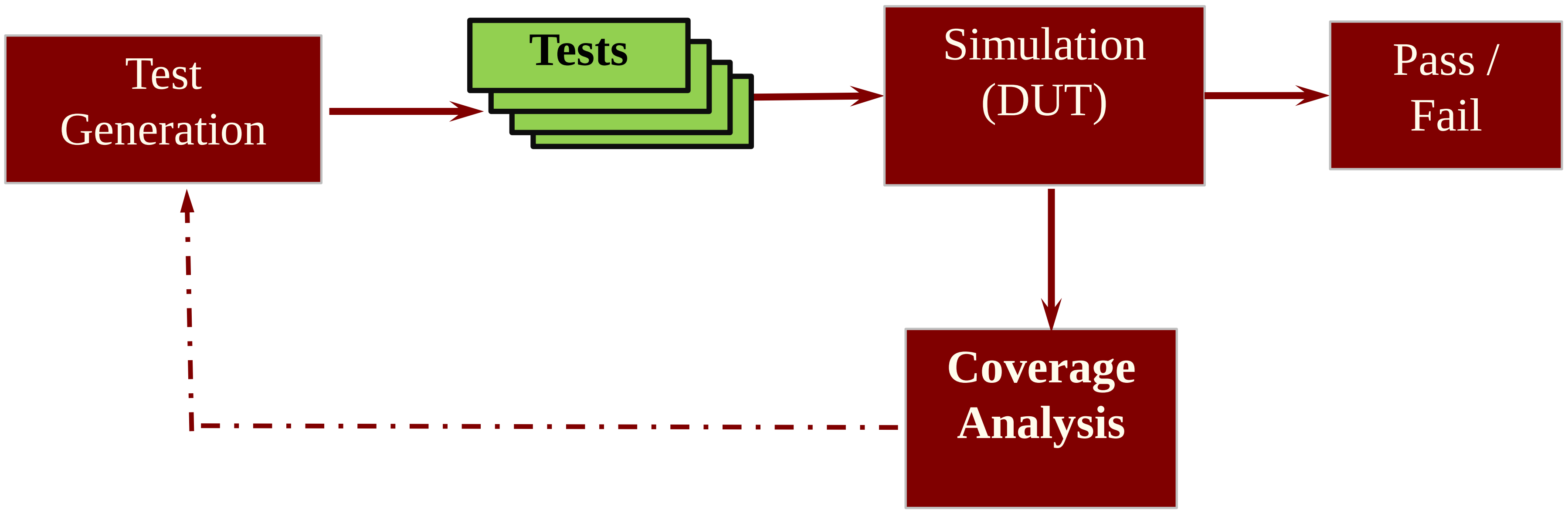
M. Chen, X. Qin, H. Koo and P. Mishra, System-Level Validation: High-Level Modeling and Directed Test Generation Techniques, Springer, 2012.

Post-Silicon Validation



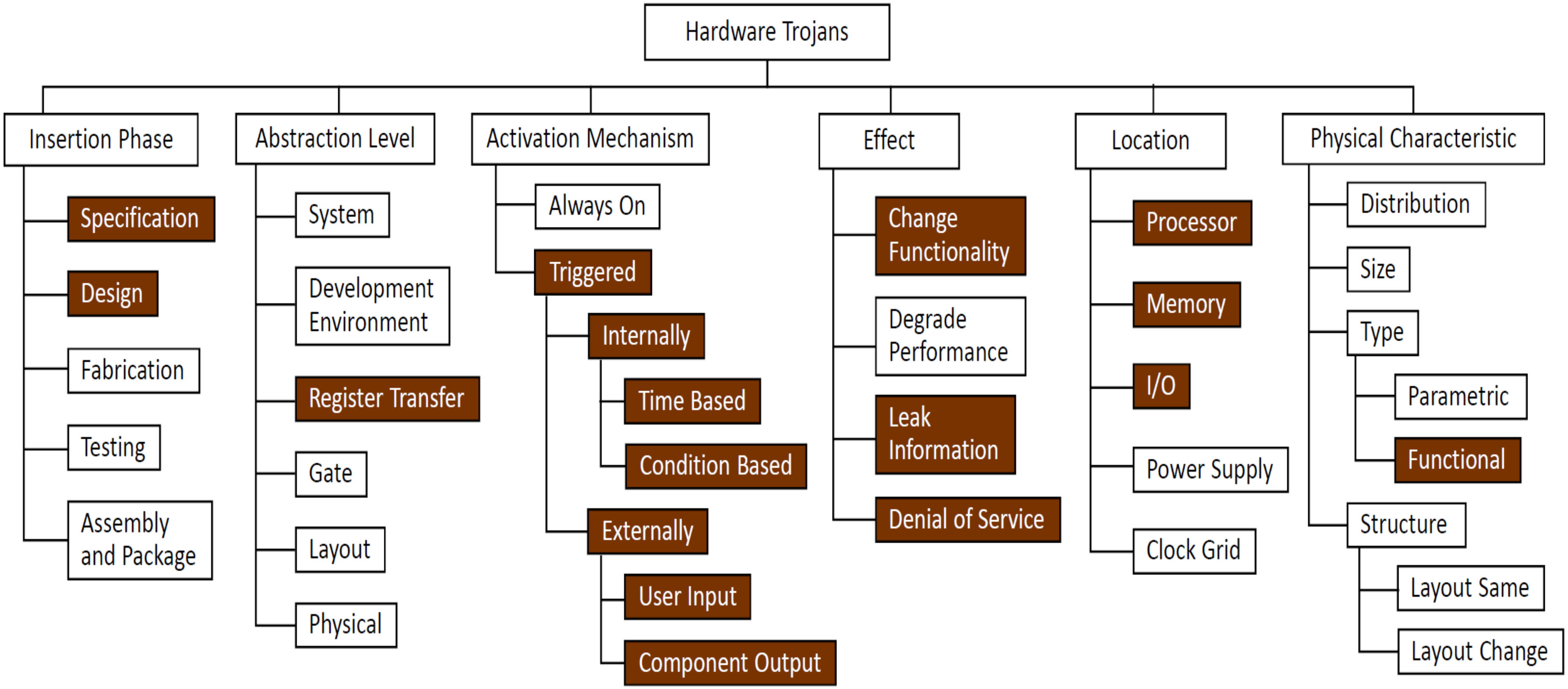
P. Mishra and F. Farahmandi (Editors), Post-Silicon Validation and Debug, Springer, 2018.

Simulation-based Validation



- Simulation-based validation is widely used
  - Uses billions to trillions of random tests
  - Still no guarantee of covering important scenarios

Threat Model



Trojan taxonomy from *www.trust-hub.org*

Trojan detectable by our approach is highlighted

A. Ahmed, F. Farahmandi, Y. Iskander and P. Mishra, Scalable Hardware Trojan Activation by Interleaving Concrete Simulation and Symbolic Execution, ITC, 2018.

Trust Metrics and Benchmarks

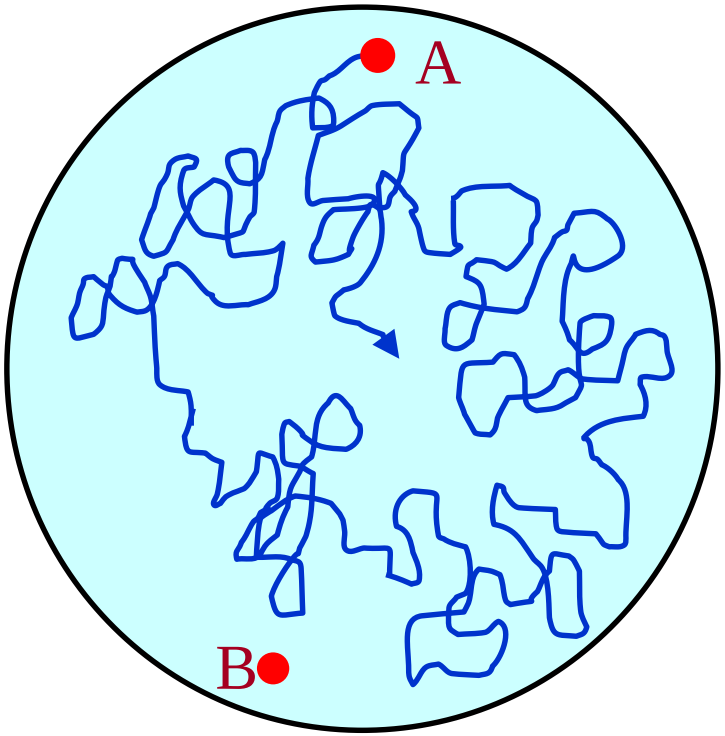
- Functional Validation
  - Code coverage (statement / branch / path)
  - FSM coverage (states and transitions)
  - Property coverage (functional scenarios)
- Parametric Validation
  - Power / thermal violations
  - Real-time violations
  - Rare-node / rare-scenario activations

Jonathan Cruz, Prabhat Mishra and Swarup Bhunia, The Metric Matters: How to Measure Trust, Design Automation Conference (DAC), 2019.

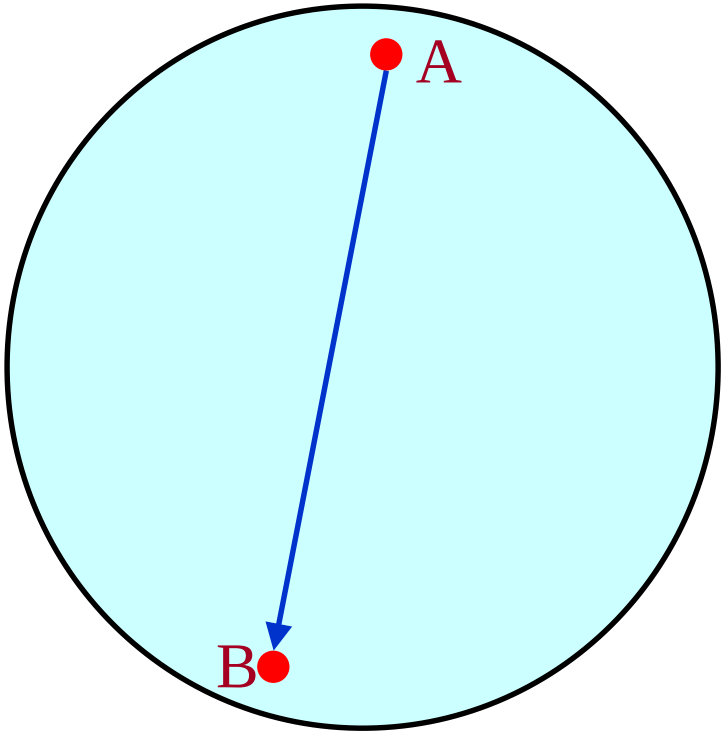
- Static and Dynamic Benchmarks

J. Cruz, Y. Huang, P. Mishra, S. Bhunia, An Automated Configurable Trojan Insertion Framework for Dynamic Trust Benchmarks, Design Automation & Test in Europe 2018.

Directed Test Generation



Random Test



Directed Test

- Significantly less number of directed tests can achieve same coverage goal than random tests
- Need for automated generation of directed tests

Y. Lyu, X. Qin, M. Chen and P. Mishra, Directed Test Generation for Validation of Cache Coherence Protocols, IEEE Transactions on CAD (TCAD), February 2018.

Test Generation using Model Checking

Example: Generate a directed test to stall a decode unit (ID)

Negated Property
(intended behavior)

assert G (ID.stall != 1)

Design

Processor Model

Model Checker

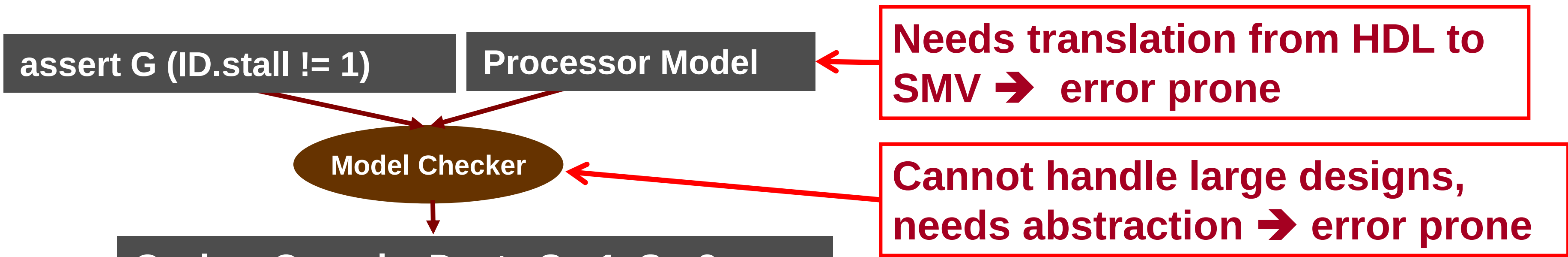
Cycle	Opcode	Dest	Src1	Src2
1	NOP			
2	ADD	R3	R1	R2
3	SUB	R4	R3	R2

Solution: Exploit learning to reduce test generation complexity

Problem: Test generation is time consuming and may not be possible when complex design and properties are involved

Scalable Directed Test Generation

- Test generation based on model checking



Cycle	Opcode	Dest	Src1	Src2
1	NOP			
2	ADD	R3	R1	R2
3	SUB	R4	R3	R2

Desirable to verify the HDL directly!

- Concolic Testing – Interleaved concrete and symbolic execution [Sen, CAV 2006]

Yangdi Lyu, Alif Ahmed and Prabhat Mishra, Automated Activation of Multiple Targets in RTL Models using Concolic Testing, Design Automation and Test in Europe (DATE), Florence, Italy, March 25 - 29, 2019.

Scalable Directed Test Generation

RTL design

Test Goal

```
module counter(out, clk, reset);
  parameter WIDTH = 8;
  output [WIDTH-1 : 0] out;
  input              clk, reset;
  reg [WIDTH-1 : 0]  out;
  wire          clk, reset;
  always @(posedge clk)
  begin
    out <= out + 1;
    if(out == 40)
      $display ("Activated");
  end
  always @reset
    if (reset)
      out = 0; // initial value
endmodule
```

Simulation

Simulation Trace

```
(out,0) = 0
(out,1) = (out,0) + 1
IF (out,0) == 40 not taken
(out,2) = (out,1) + 1
IF (out,1) == 40 not taken
(out,3) = (out,2) + 1
IF (out,2) == 40 not taken
```

```
(out,1) = (out,0) + 1
(out,0) != 40
(out,2) = (out,1) + 1
(out,1) != 40
(out,3) = (out,2) + 1
(out,2) = 40
```

Constraint Solver

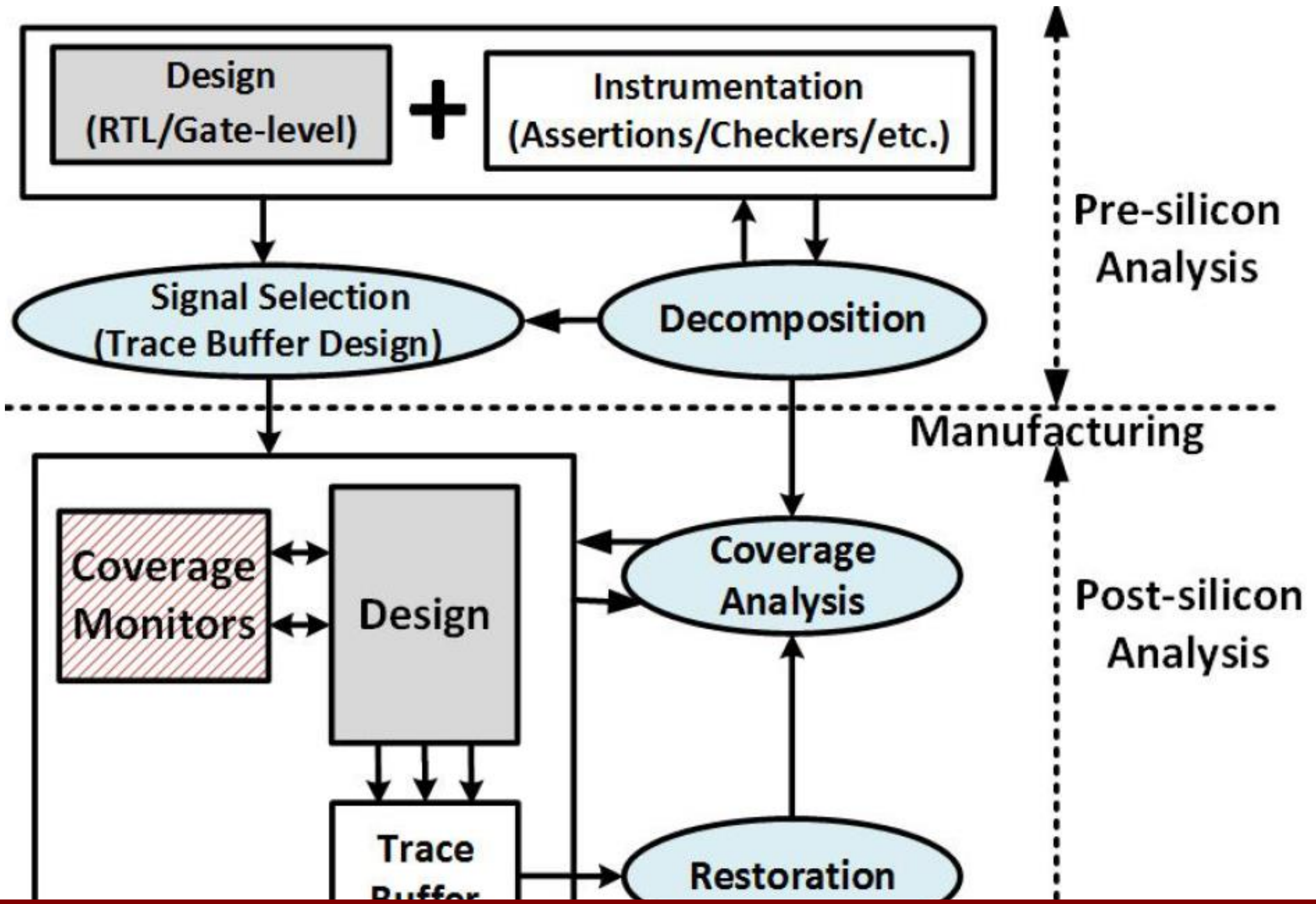
(out,0) = 38

Test

Constraints

A. Ahmed, F. Farahmandi and P. Mishra, Directed Test Generation using Concolic Testing of RTL Models, Design Automation and Test in Europe (DATE), 2018.

Assertion-based Validation



F. Farahmandi, R. Morad, A. Ziv, Z. Nevo and P. Mishra, Cost-Effective Analysis of Post-Silicon Functional Coverage Events, Design Automation and Test in Europe (DATE), 392-397, 2017.

Outline

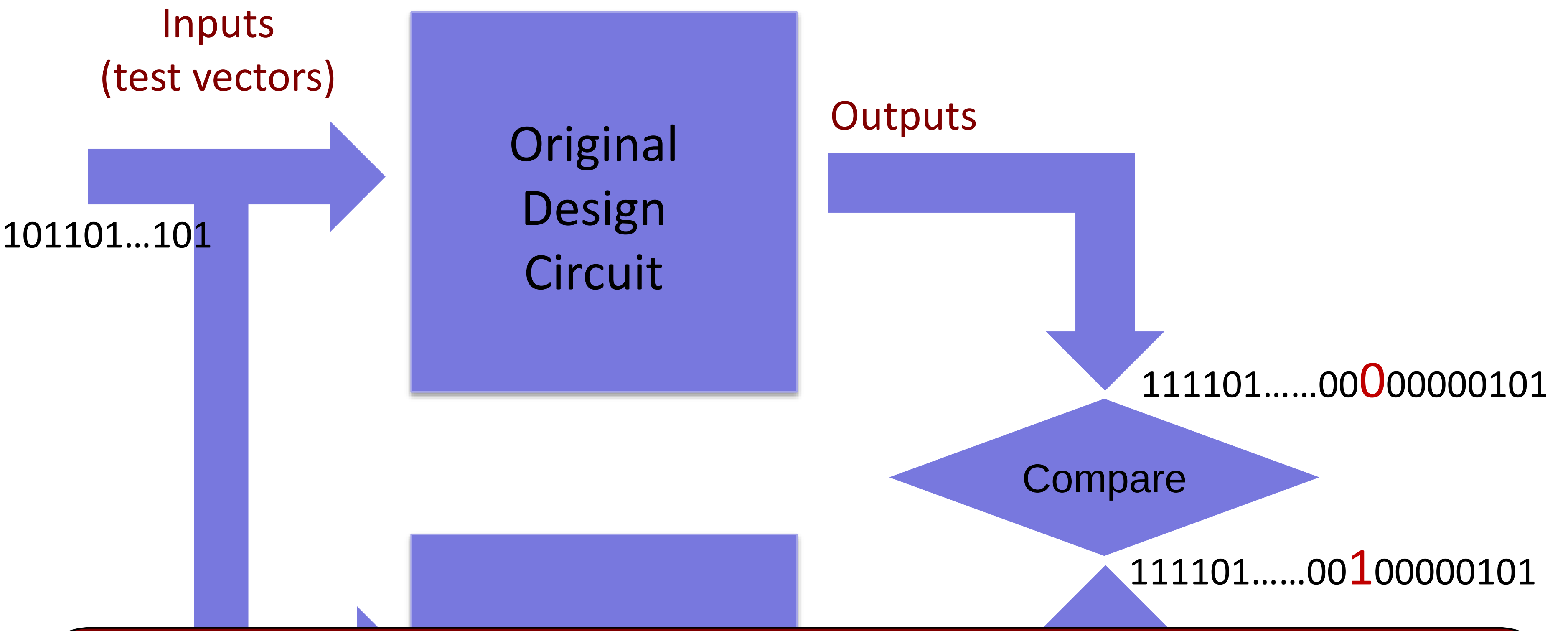
- Introduction
- Design for Security
- Security Attacks and Countermeasures
- Security and Trust Validation
  - Simulation-based Security Validation
  - Security Validation using Side Channel Analysis
  - IP Trust Validation using Formal Methods
- Application-Specific Security
- Conclusion

HW Trojan Detection

	Logic Testing	Side-Channel Analysis
Pros	• Robust under process noise • Effective for ultra-small Trojans	• Effective for large Trojans • Easy to generate test vectors
Cons	• Difficult to generate test vectors • Large Troj. detection challenging	• Vulnerable to process noise • Ultra-small Troj. Det. challenging

Y. Huang, S. Bhunia and P. Mishra, MERS: Statistical Test Generation for Side-Channel Analysis based Trojan Detection, ACM Conference on Computer and Communications Security (CCS), pages 130-141, 2016.

Logic Testing for Trojan Detection



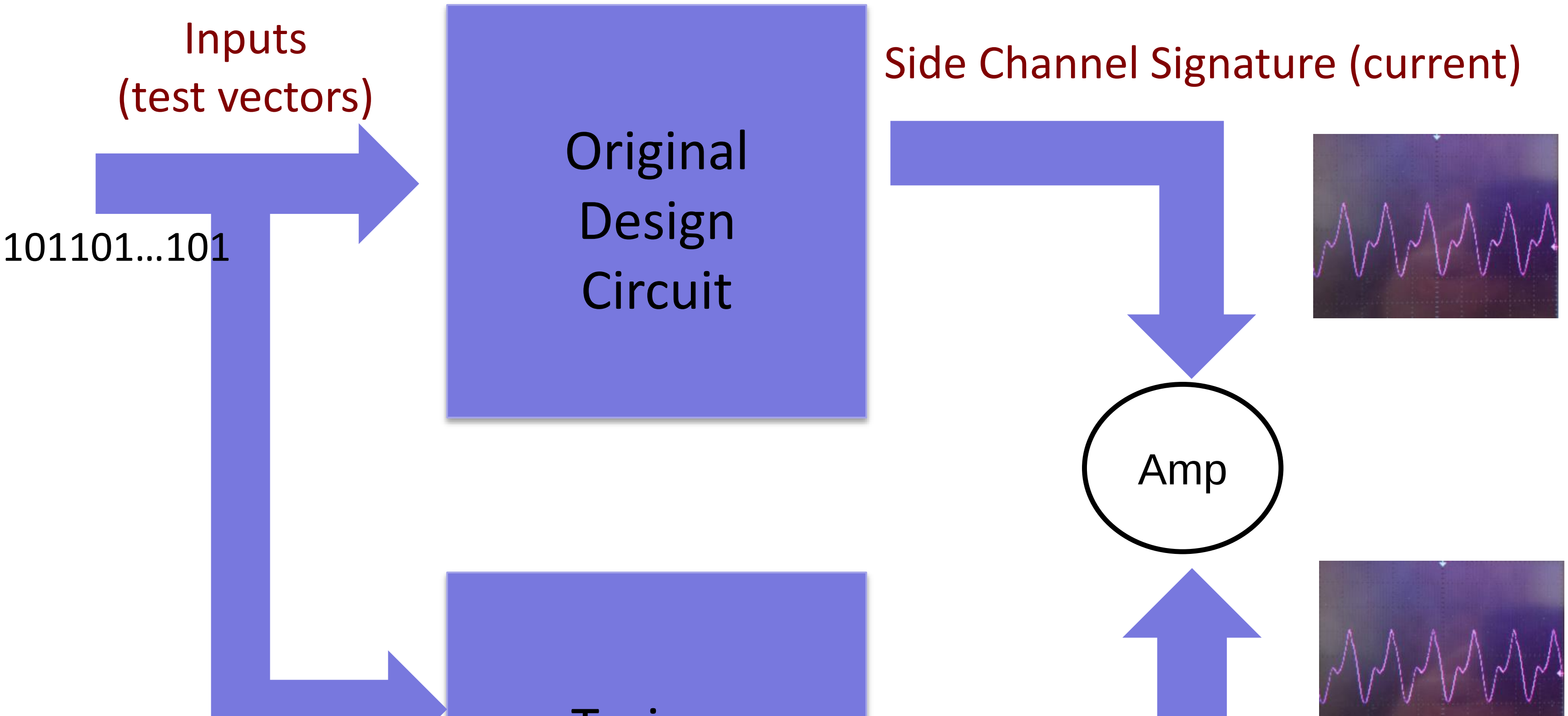
Not effective:

(1) Test space (no way to cover all inputs and all circuit states)

(2) Trojan space (unknown locations, unknown triggers)

(3) Trojan is stealthy (rare triggering)

Side Channel Analysis (SCA) for Trojan Detection

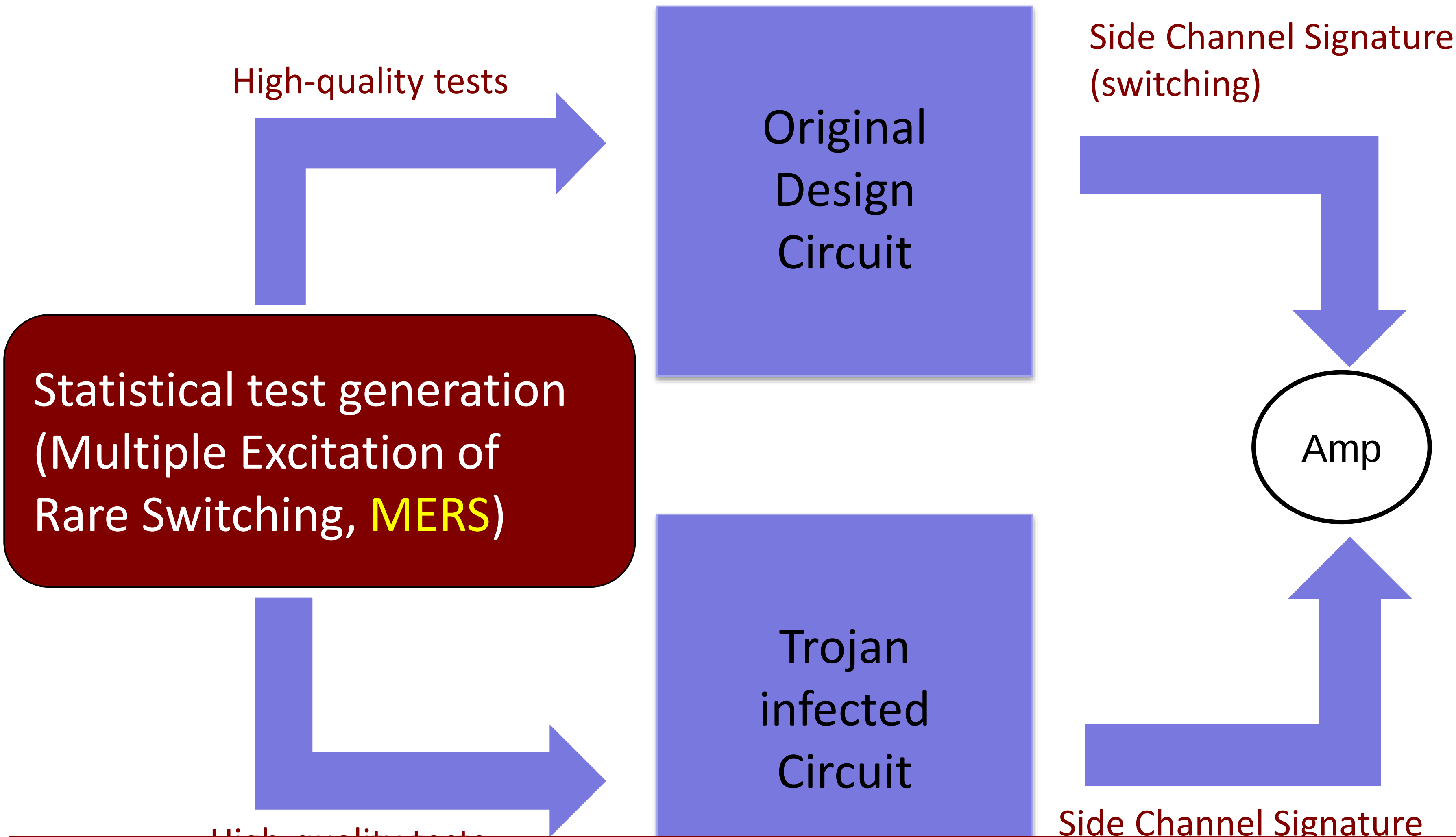


Not effective:

(1) Trojan is small and dormant (different of signature is small)

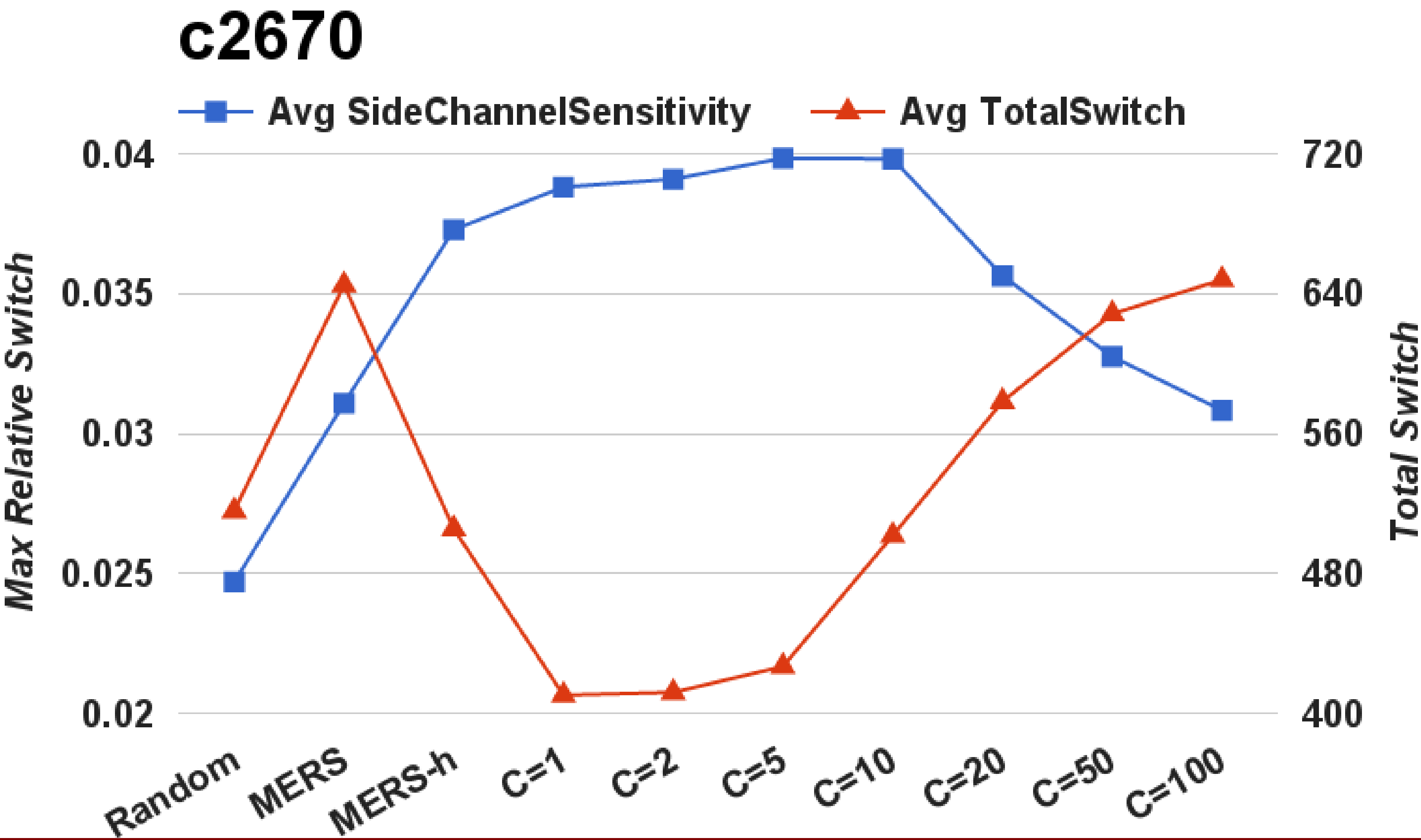
(2) Sensitivity (process noise and background switching)

Our Approach: Logic Testing + SCA



Y. Huang, S. Bhunia, P. Mishra, Scalable Test Generation for Trojan Detection using Side Channel Analysis, IEEE Trans. on Information Forensics & Security (TIFS), 2018.

Effect of Weight Ratio (C)



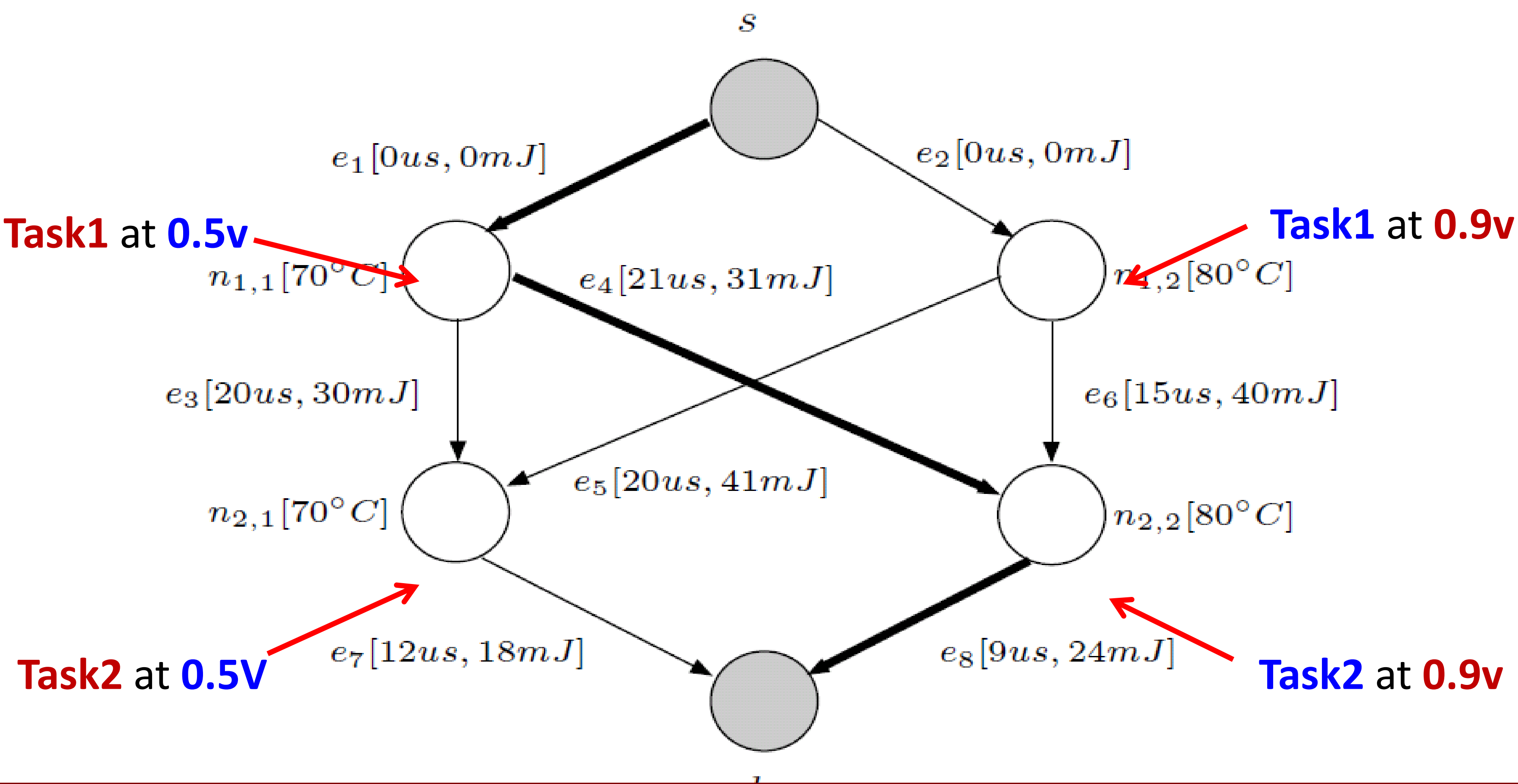
Y. Huang, S. Bhunia P. Mishra, MERS: Statistical Test Generation for Side-Channel Analysis based Trojan Detection, ACM Conf. on Computer and Communications Security (CCS), 2016.

Outline

- Introduction
- Design for Security
- Security Attacks and Countermeasures
- Security and Trust Validation
  - Simulation-based Security Validation
  - Security Validation using Side Channel Analysis
  - IP Trust Validation using Formal Methods
- Application-Specific Security
- Conclusion

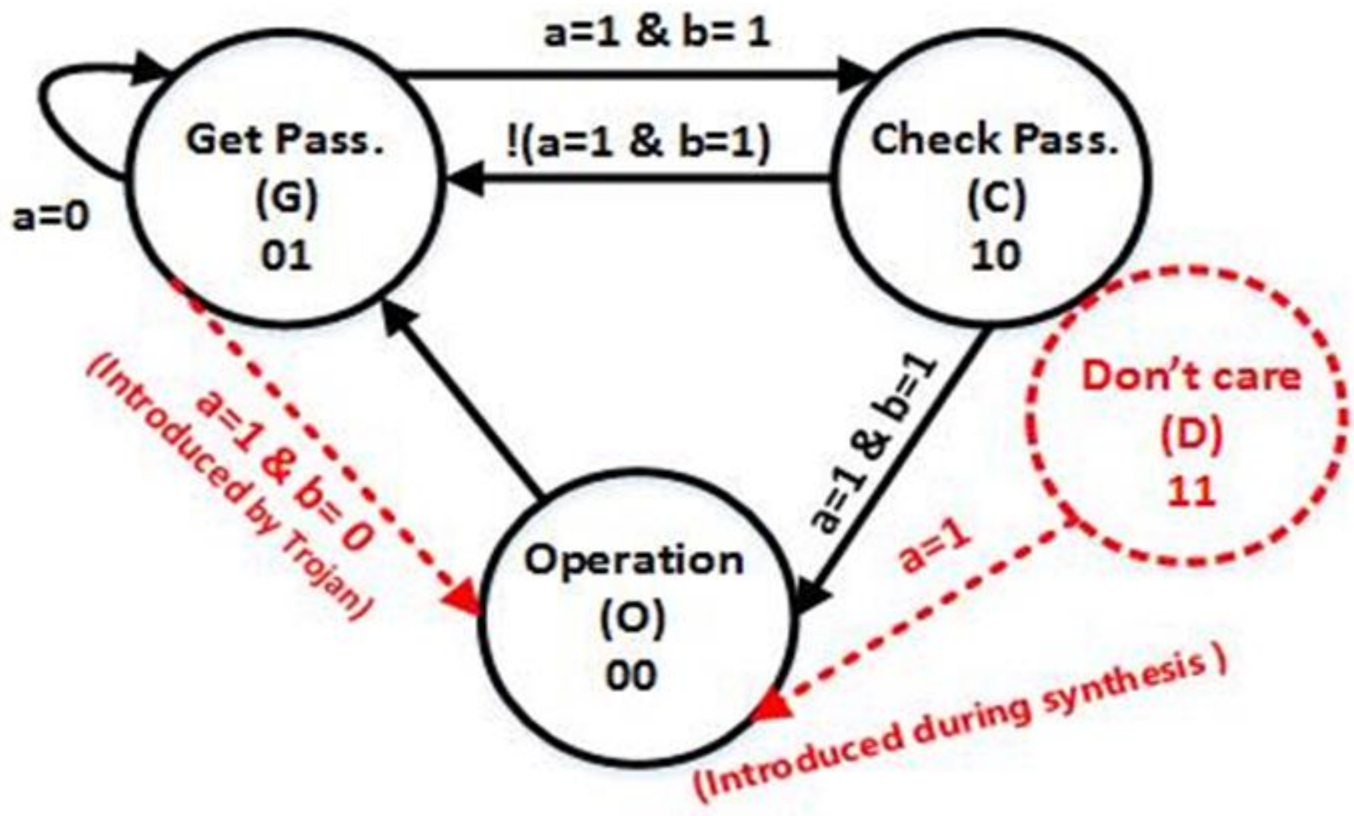
Checking Non-functional Properties

- Find a path that satisfies a specific property



X. Qin, W. Wang and P. Mishra, Temperature- and Energy-Constrained Scheduling in Real-Time Multitasking Systems, IEEE Transactions on CAD (TCAD), 2012.

FSM Anomaly Detection

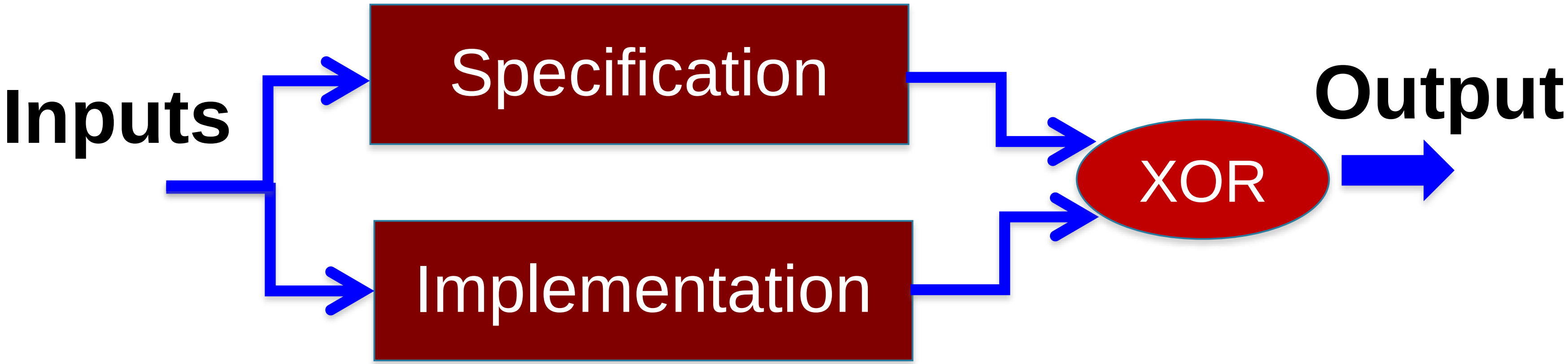


A. Nahiyan et al., Security-aware FSM Design Flow for Identifying and Mitigating Vulnerabilities to Fault Attacks, IEEE Transactions on CAD (TCAD), 2018.

F. Farahmandi and P. Mishra, FSM Anomaly Detection using Formal Analysis, IEEE International Conference on Computer Design (ICCD), 2017.

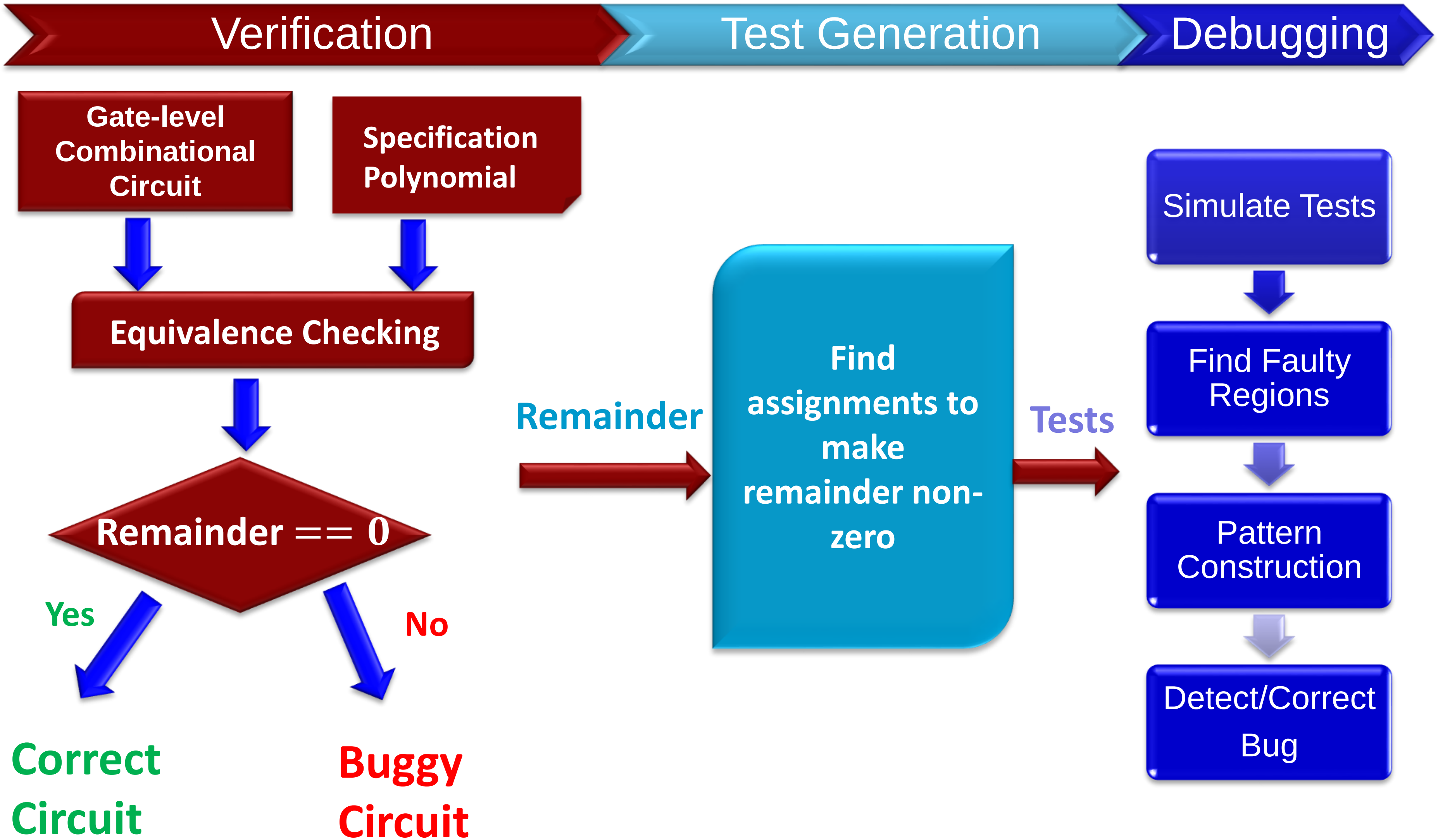
Equivalence Checking

- Traditional Equivalence Checkers
- Equivalence Checking using SAT Solvers



- Does not work for industrial designs unless the design structure (FSM) is similar

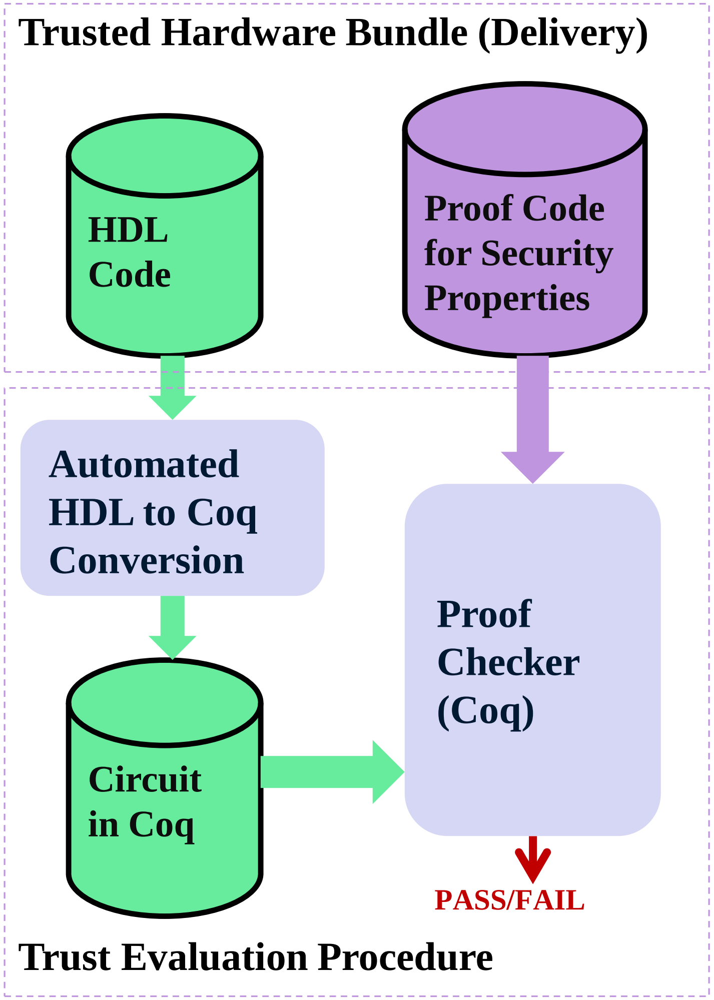
Automated Detection and Correction



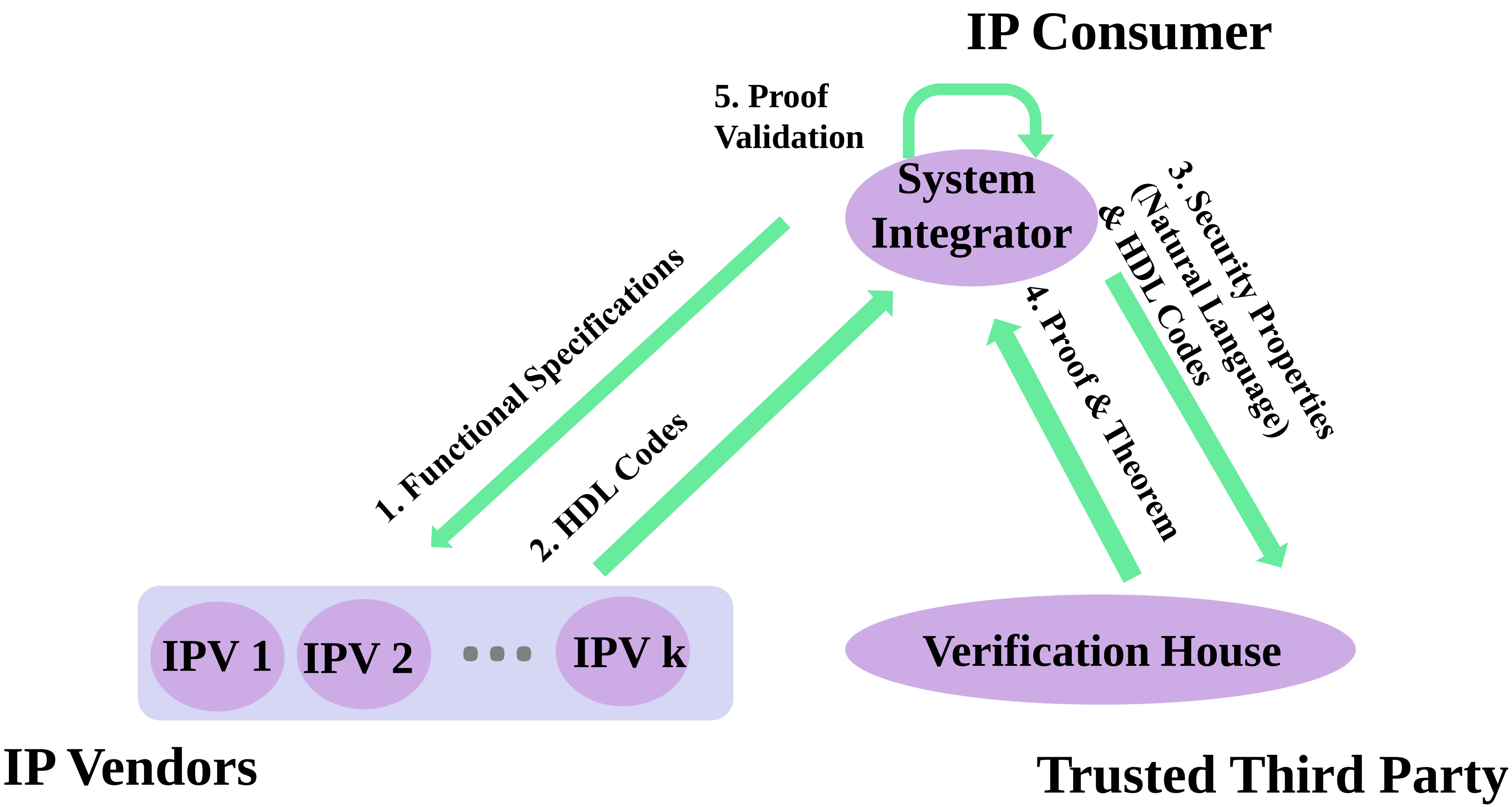
F. Farahmandi and P. Mishra, Automated Test Generation for Debugging Multiple Bugs in Arithmetic Circuits, IEEE Transactions on Computers (TC), 68(2), 182-197, 2019.

Proof-Carrying Hardware IP Cores

- Trusted IP Acquisition (consumers)
  - User receives IP code AND a formal proof regarding the code's trustworthiness
  - Existence of Proofs certify verification of HDL code against security properties
  - Proofs are validated automatically and efficiently by the proof checker in Coq
  - Unlike functional specifications, security properties concern both functionality and information sensitivity



Working Procedure – Main Parties



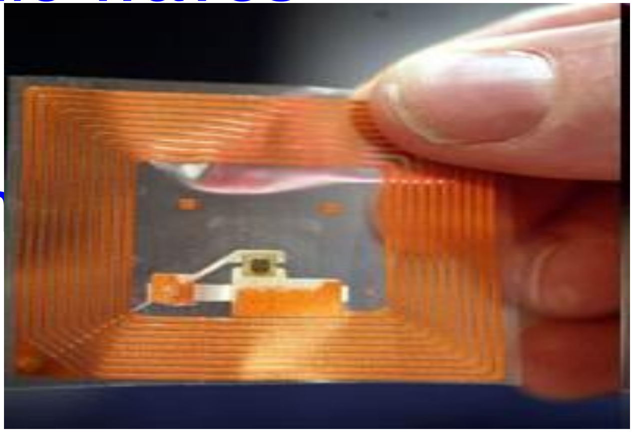
X. Guo, R. Dutta, P. Mishra and Y. Jin, Automatic Code Converter Enhanced PCH Framework for SoC Trust Verification, IEEE Transactions on VLSI, December 2017.

Outline

- Introduction
- Design for Security
- Security Attacks and Countermeasures
- Security and Trust Validation
- Application-Specific Security
- Conclusion

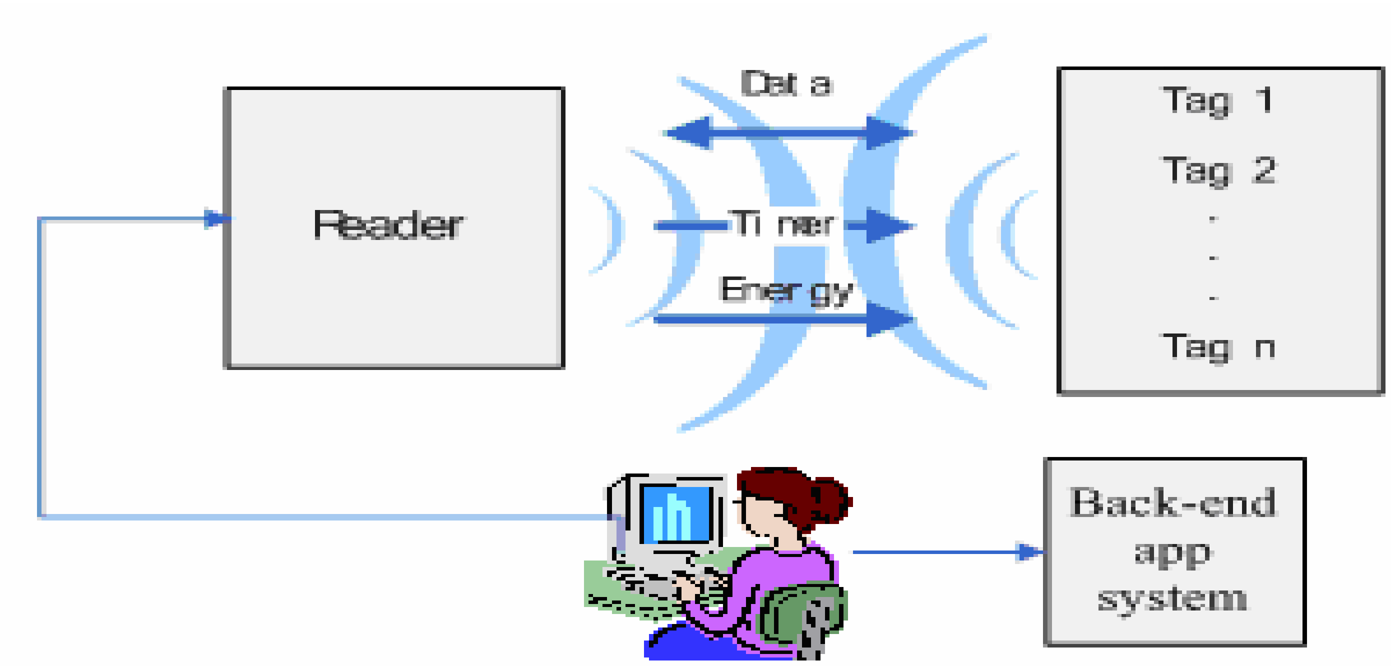
RFID

- Radio frequency identification (RFID) is an automatic identification method
  - Retrieve and access data using RFID tags
  - RFID tags are intelligent bar codes that can talk to a networked system which can track and identify every product using radio waves
- RFID system includes:
  - Tags, readers, database systen



RFID System

- RFID system includes:
  - Tags, readers, database system



Attacks for Impersonation

1. Tag Cloning

- Duplicating or manipulating RFID tag data to make similar copies that can be accepted by an RFID application as valid
- In simple passive RFID systems, cloned tags are indistinguishable from authentic ones

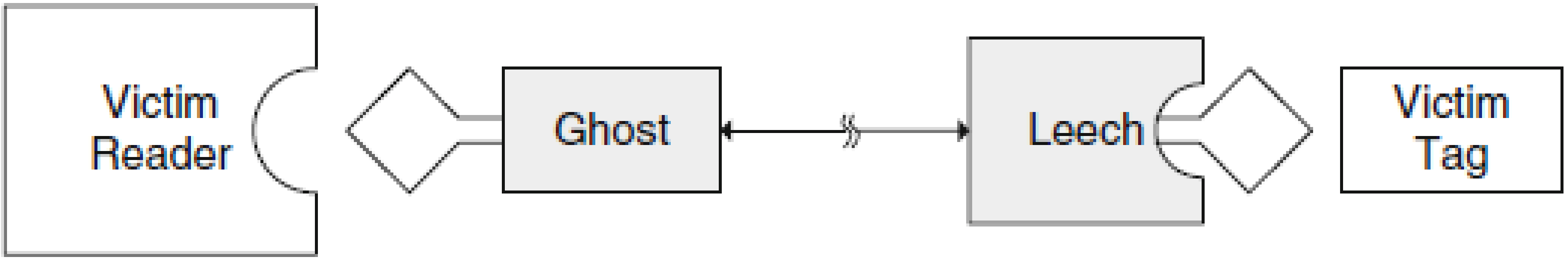
2. Tag Spoofing (emulation)

- May use custom designed electronic device to imitate, or emulate, the authentic tag
- Can fool automated checkout system into thinking product is still on shelf
- Adversary must have full access to legitimate communication channels and knowledge of protocols

Attacks for Impersonation

3. Relay Attacks

- Need two devices acting as a tag and a reader
  - Leech device as reader to legitimate tag
  - Ghost device as tag to legitimate reader
- The illegitimate devices can modify the data during relay
- Can be carried out over considerable distances



Attacks for Impersonation

4. Replay Attacks

- Similar to relay attack
- May use captured valid reader-tag communication data at a later time
  - Use for other readers or tags for impersonation
- Data can be captured via relay attacks or eavesdropping
- Typical scenario involved breaking RFID-based access control systems

Attacks for Information Leakage

1. Eavesdropping

- Attacker uses special reader and antennas to collect an RFID data.
- Records the messages in either direction
  - Forward channel → reader-to-tag
  - Backward channel → tag-to-reader

2. Code Injection Attacks (Tag Modification)

- Data contained in the RFID tag can be modified so that it contains malicious code which can change the course of execution of backend systems or databases processing the RFID data
- i.e. adversary may wipe out price stored on tags for expensive products in a store – write a cheaper price to it

The Reality of Car Hacks

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

BMW, Audi and Toyota cars can be unlocked and started with hacked radios

The affected cars include BMW's 730d, as well as models from Audi, Honda, Ford and Toyota. CREDIT: RICHARD NEWTON

Researchers Show How to Steal Tesla Car by Hacking into Owner's Smartphone

Friday, November 25, 2016 Mohit Kumar

The Infrastructure Hacks

Tuesday, February 3, 2009

Zombie Road Signs Invading Australia (No Joke)

" 'Zombie' copycats hack electronic road signs"
News.com.au (February 3, 2009)

"ZOMBIE road signs are invading Australia, as vandals take to hacking the electronic displays with simple instructions from the web.

" 'Zombies ahead!' warned one sign on the Gold Coast this week, in reference to a now-infamous message displayed in the US last month.

"The pranksters also illegally hacked into signs around the area with other messages, including "Nobody has ever loved you," according to GoldCoast.com.au...."

No question about it: there's humor in these hacked road signs. I indulged in a chuckle, myself.

It's funny.

Until somebody gets killed. These are working road signs, remember?

L.A. NOW

SOUTHERN CALIFORNIA -- THIS JUST IN

« Previous Post | L.A. NOW Home | Next Post »

'Anonymous' hackers target BART, Fullerton police

AUGUST 14, 2011 | 2:31 PM

CYBERSECURITY February 12, 2008

Teen Hacker in Poland Plays Trains and Derails City Tram System

Automotive Security and Privacy

SEAMLESS CONNECTED MOBILITY EXPERIENCE	ADVANCED DRIVER ASSISTANCE → SELF-DRIVING	ENERGY EFFICIENCY
		
Enjoying life one hour per day	Enhance and replace driver functions	Make driving environment friendly

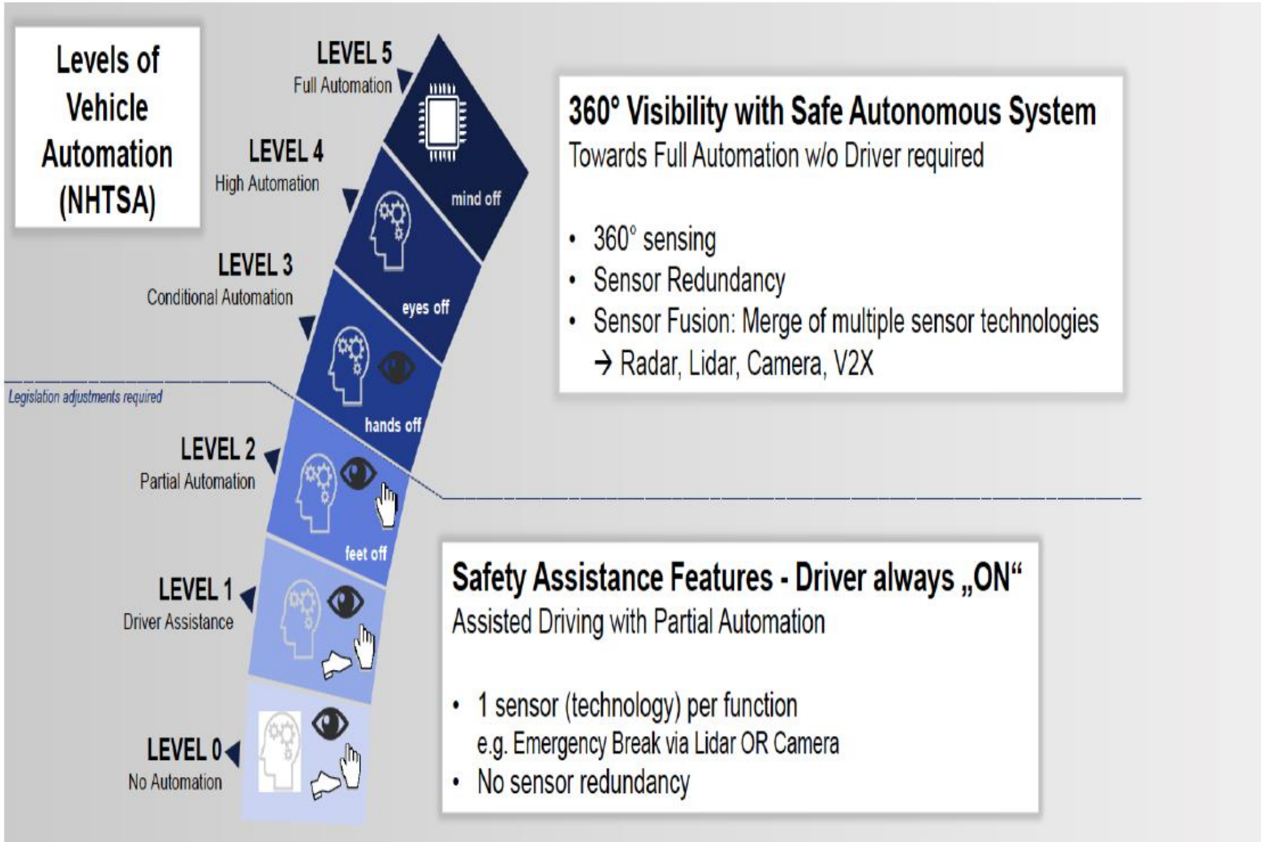
SW and electronics represent key market distinction for a modern car

A modern automobile has ~100 processors (Electronic Control Units), 2 miles of cable, several hundred MB of software, and 3-5 in-vehicle networks

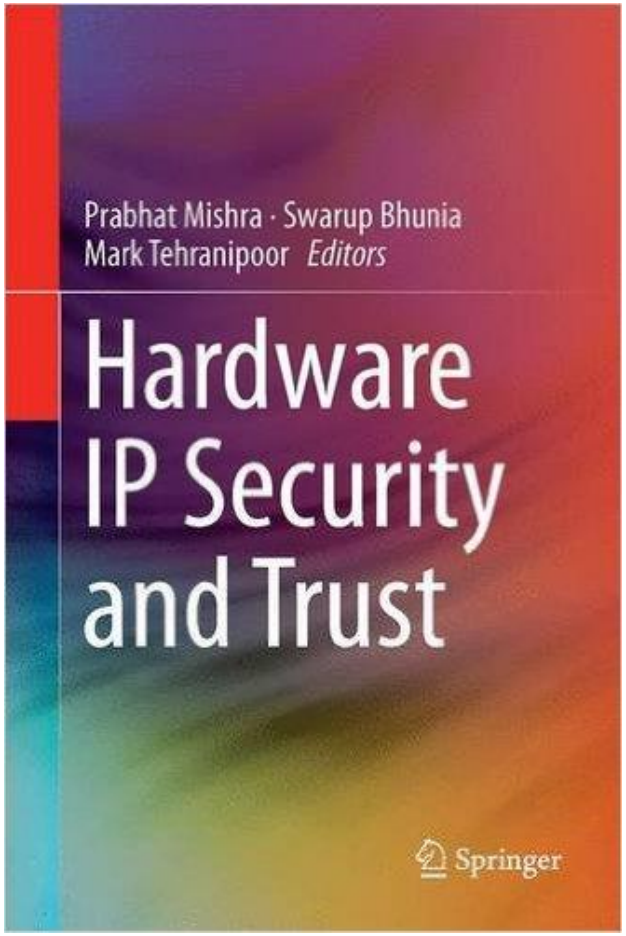
Tomorrow's Autonomous Vehicles

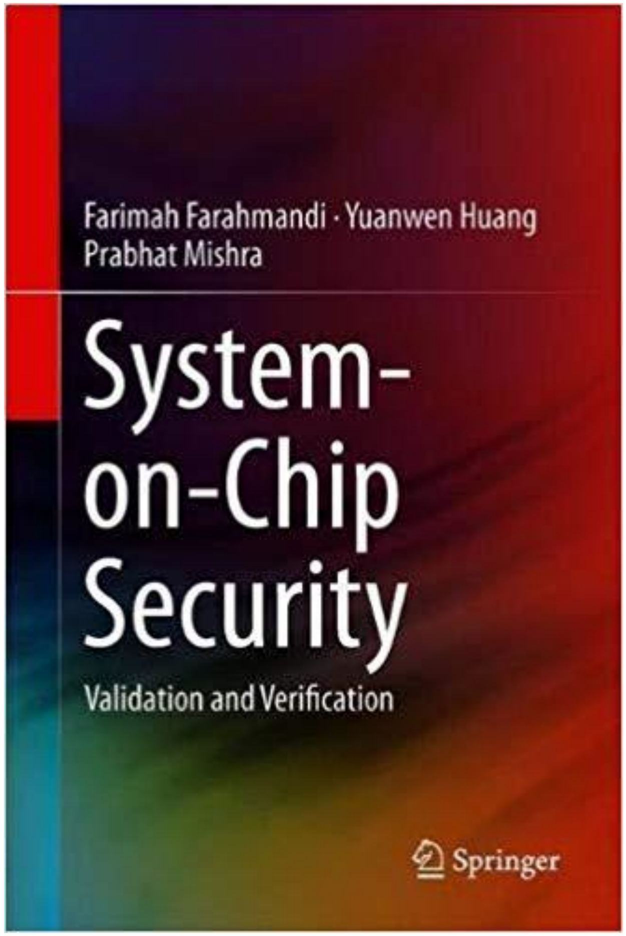
China Race to Develop Autonomous Vehicles, NewSecurityBeat, February 28, 2019

Much more to come …



Thank you!





prabhat@ufl.edu

http://www.cise.ufl.edu/~prabhat