UNIVERSITY OF MARYLAND 1856

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

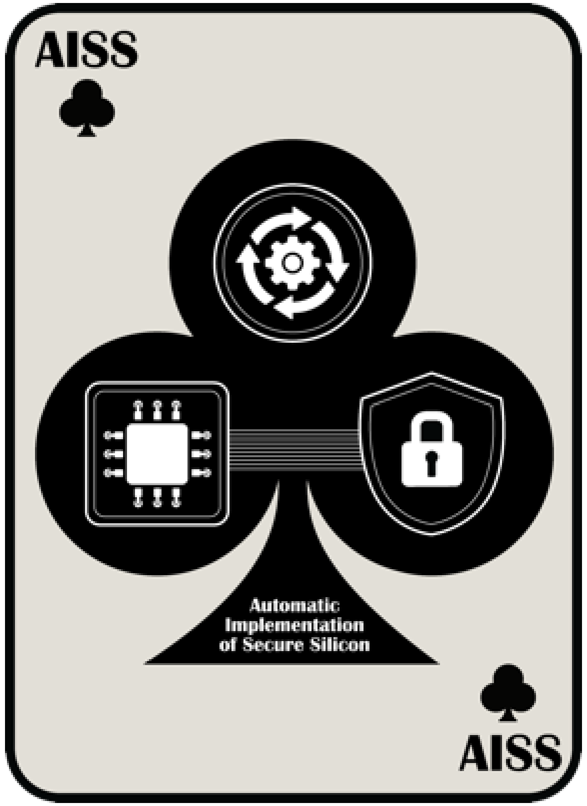
Protecting Your Chip From Attackers

Warren Savage

EDPS Conference, October 6, 2023

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

AISS - Democratizing Security



Source: DARPA AISS Proposers Day, April 2019

Problem Statement

- Threats are increasing
- IOT increases attack surface
- Few security experts in semiconductor
- Expensive to design

Solution

- Embed expertise into flow
- New EDA tools
- New IP

Cost Function Examples

Application	Perf.	Size	Power	Security
Lawn Sprinkler	2	7	9	1
Engine Control	6	5	1	3
Guided Projectile	5	1	9	7
Network Router	9	5	1	8
Mobile Phone	7	9	9	7
Smart Watch	3	6	9	3

Security Cost Function Expansion

Application	Side Channel	Reverse Eng'g	Supply Chain	Malicious Hardware
Lawn Sprinkler	1	1	9	1
Engine Control	1	7	5	2
Guided Projectile	3	9	5	9
Network Router	9	7	8	9
Mobile Phone	8	9	9	6
Smart Watch	6	8	9	1

Types of (hardware) Attacks

Side Channel

- Extraction of secrets through communication channels other than intended

Motivation	
Economic Gain	
IP Theft	✓
Sabotage	
Espionage	✓

Reverse Engineering

- Extraction of algorithms from an illegally obtained design representation

Motivation	
Economic Gain	✓
IP Theft	✓
Sabotage	
Espionage	✓

Hardware Trojans

- Insertion of secretly triggered hidden disruptive functionality

Motivation	
Economic Gain	
IP Theft	
Sabotage	✓
Espionage	✓

Supply Chain

- Cloning, counterfeit, recycled or re-marked chips represented as genuine

Motivation	
Economic Gain	✓
IP Theft	
Sabotage	
Espionage	

Blue Team vs Red Team roles

Defend

- Identify vulnerabilities
- Develop defenses

Synopsys® Northrop Grumman

Attack

- Find vulnerabilities
- Attack defenses

Applied Research Laboratory for Intelligence and Security

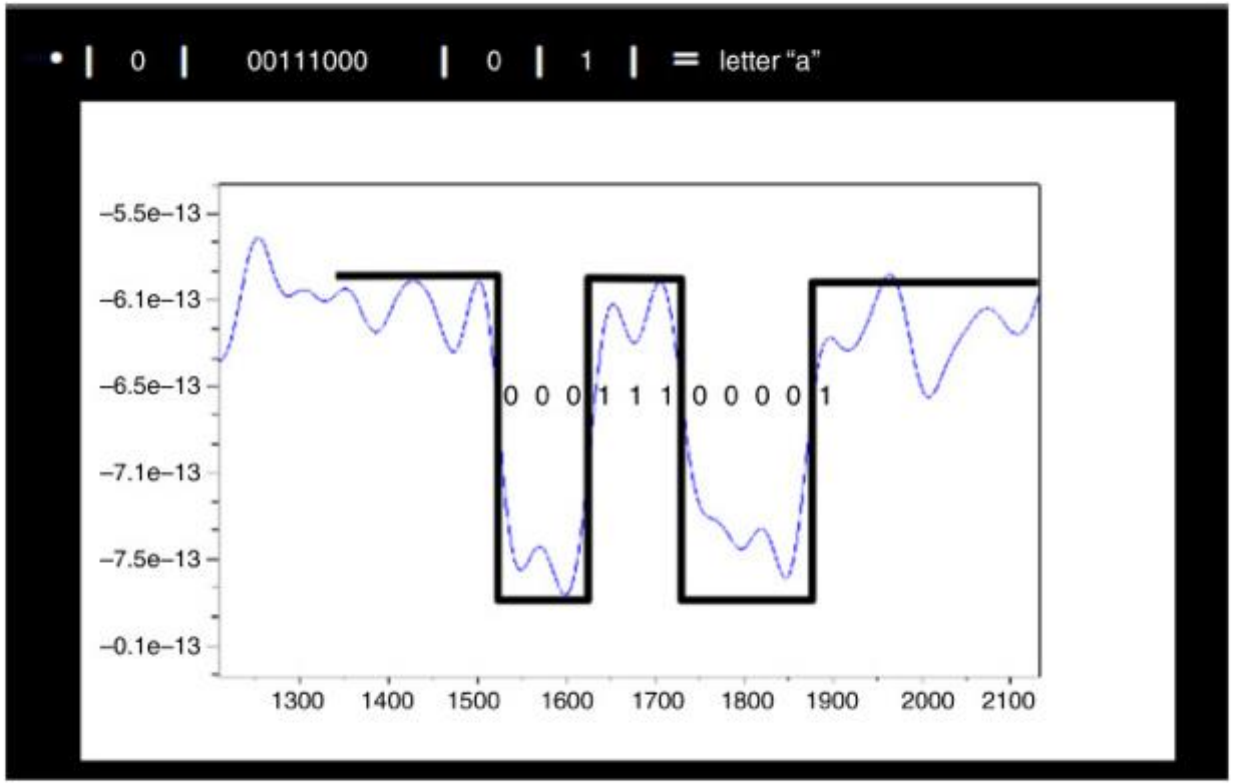
APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Side Channel Attacks

Types of Side Channel Attack

- Extraction of Information from a weakness in the implementation
  - Typically cryptographic keys or algorithms or other high value items
- Methods of attack to discern secrets
  - Power – monitoring power consumption
  - Timing – monitoring timing variations
  - Electromagnetic – monitoring emissions
  - Optical – using advanced imaging to discover implementation

The letter "A" detected by measuring ground noise



University of Florida
Florida Institute for Cybersecurity Research

Power Side Channel Analysis at the Pre-silicon Stage

AES-128 RTL Code

→

1. Synthesis

Tool: Design Compiler
Input: Design Data (.v,.vhd files)
Output:
Gate-level Netlist
Net/Cell Parasitic

→

2. Acquiring Switching Activities

Tool: VCS Simulator
Input: Gate-level Netlist, Design Testbench
Output:
Switching Activity file (.vcd)

→

3. Time-based Power Simulation

Tool: PrimePower
Input: Gate-level Netlist, Switching Activity File, Cell/Net Parasitic
Output:
Time-based Power Reports (.out, .fsdb)

↓

4. Processing Power Traces

Tool: IV&V SCA-Red tools
Input: Design Data (.out, .fsdb)
Output:
Synchronized Stackable Power Traces (.npy)

←

5. Conformance Style Testing

Tool: IV&V SCA-Red TVLA tool
Input: Synchronized Power Traces (.npy)
Output:
Leaky design?

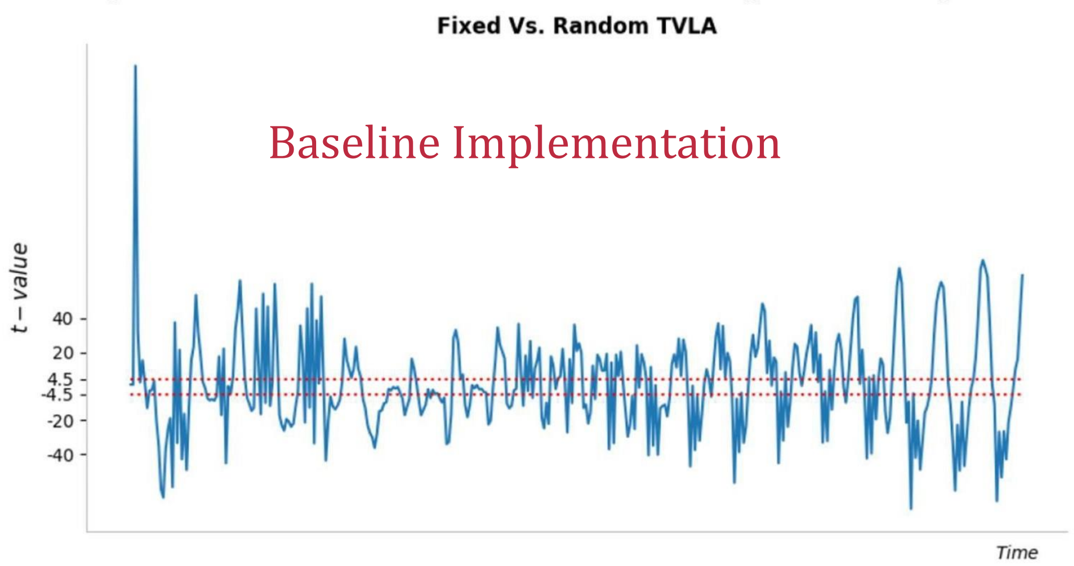
←

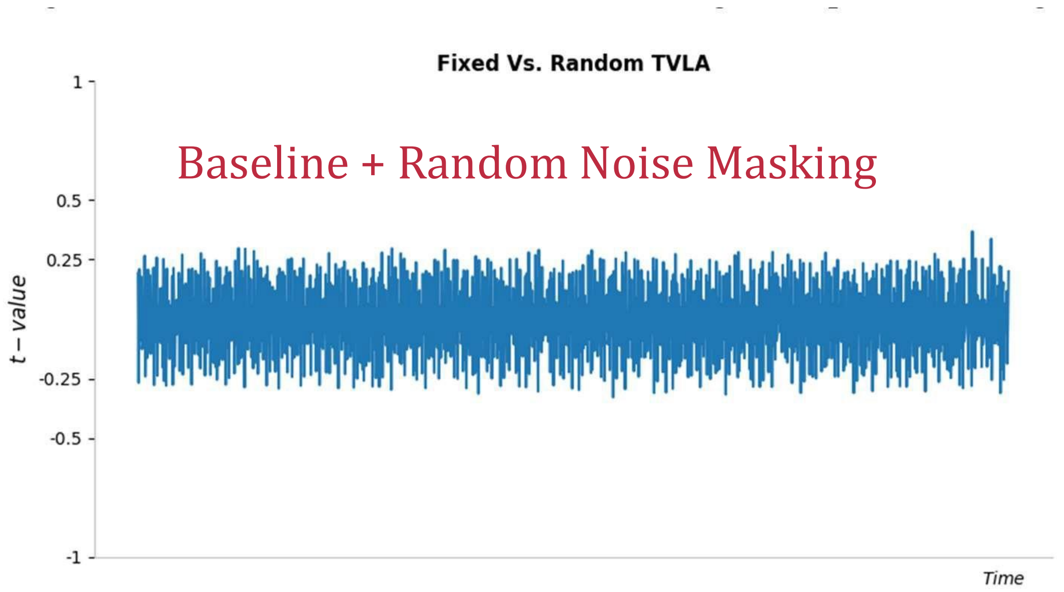
6. Evaluation Style Testing

Tool: JuliaSCA for CPA
Input: Synchronized Stackable Power Traces (.npy)
Output:
Key Material

The 128-bit key of is revealed successfully from the power trace of 10,000 encryptions!

AES-128 Results (Step 5)





Implementation	2000 traces t-value	Area (32nm)	Area Penalty (%)
Baseline	188.6σ	65,179 μm^2	0
+ High Freq. noise	0.93σ	111,481 μm^2	71%
+ Random noise	0.32σ	271,086 μm^2	316%

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

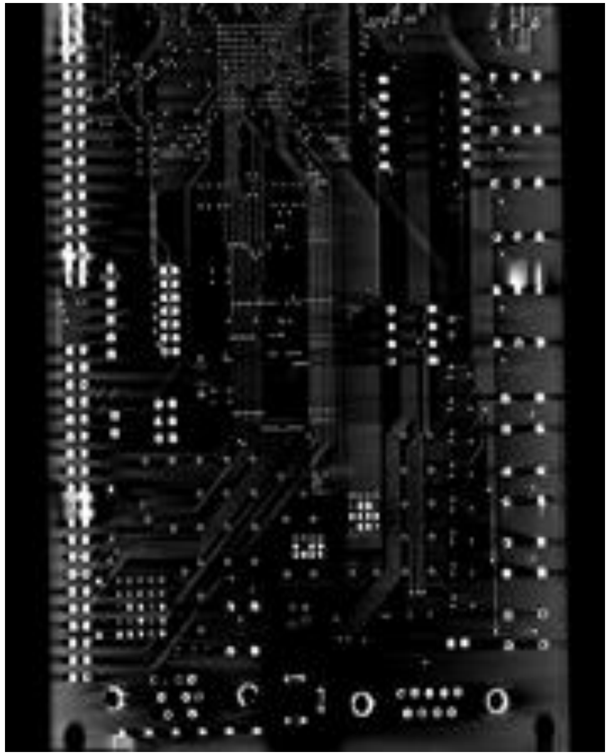
UNIVERSITY OF MARYLAND 1856

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Reverse Engineering Attacks

Reverse Engineering X-ray Attack on a 6-layer PCB

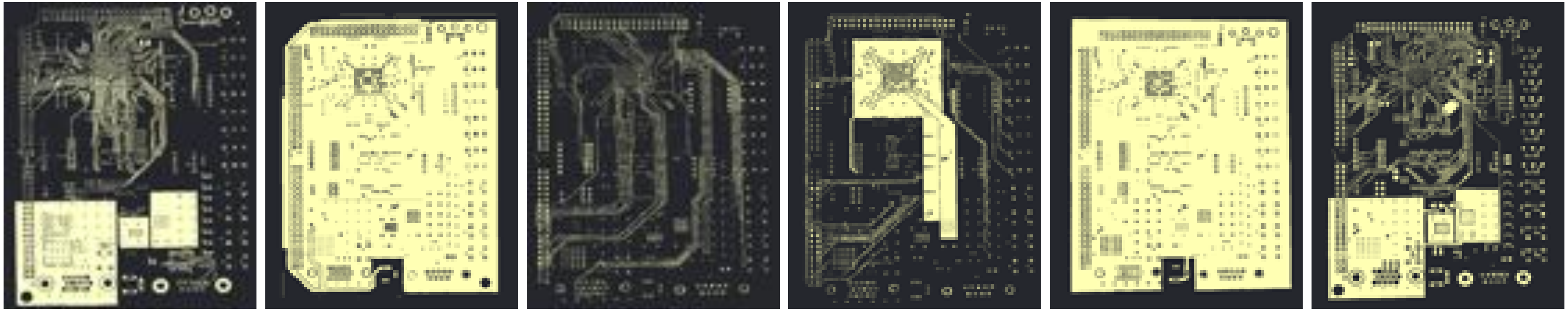
Inner layer



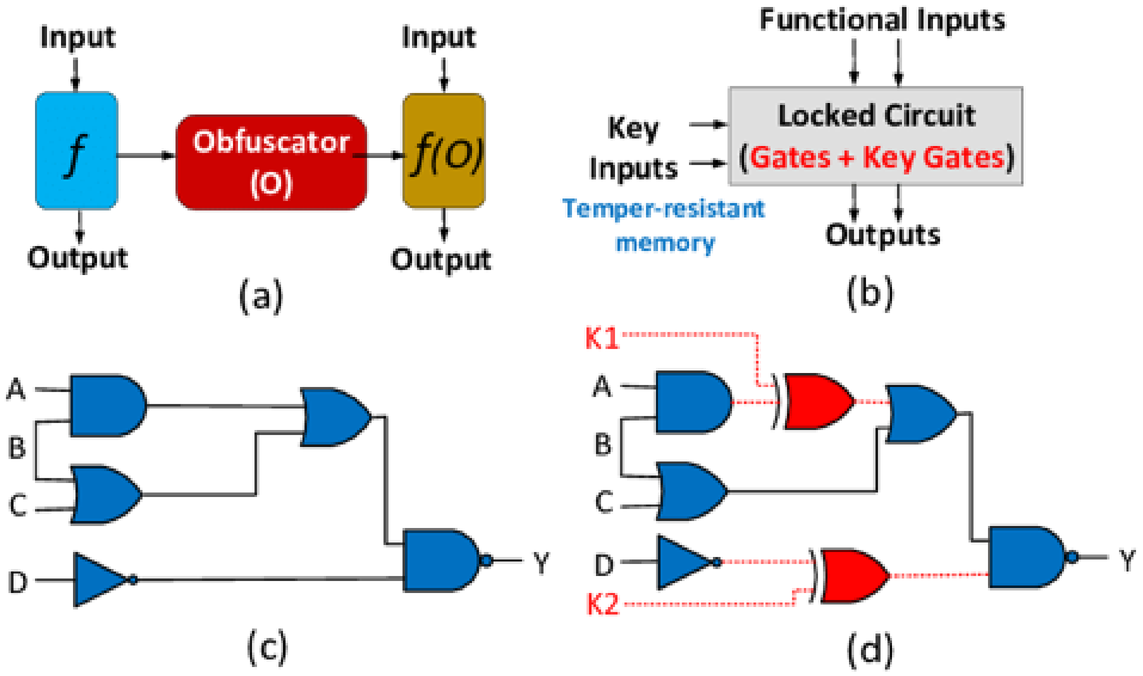
Top layer

University of Florida
Florida Institute for Cybersecurity Research

Reverse Engineering CT Scan Attack on same 6-layer PCB



Protecting a Circuit through Obfuscation or Locking



Chip Owner	Design	
EDA Tool	Obfuscation	
Outsourced	Foundry	Nonfunctional Silicon
Outsourced	OSAT	Nonfunctional Silicon
Chip Owner	Activation	Functional Silicon

Source: Conference Paper: Deep RNN-Oriented Paradigm Shift through BOCANet: Broken Obfuscated Circuit Attack
Tehranipoor, Fatemeh & Karimian, Nima & Kermani, Mehran & Mahmoodi, Hamid. (May 2019)

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

Attacks on Logic-Locked/Obfuscated Designs

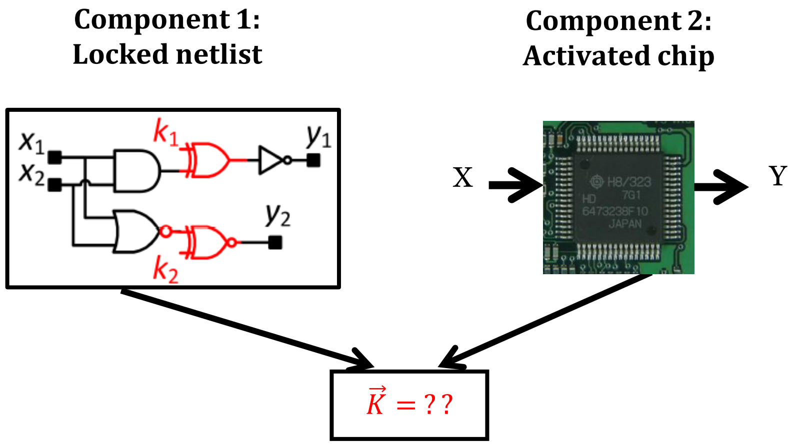
Logic-based attacks

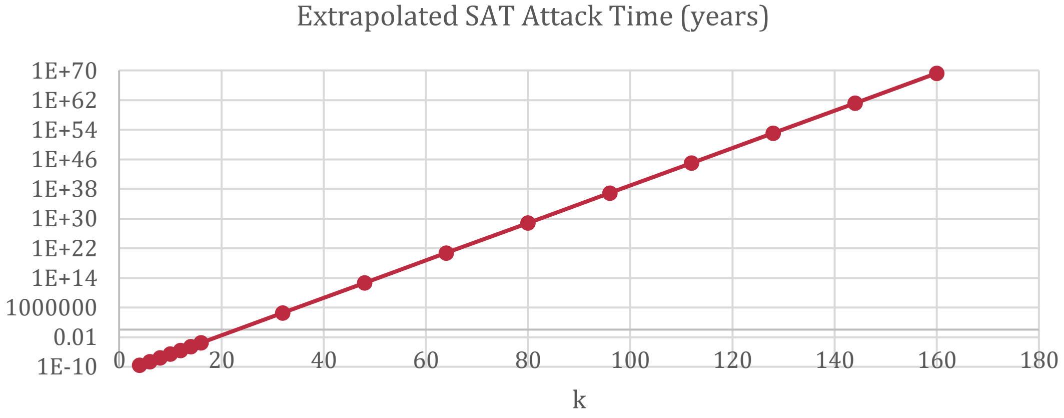
- Boolean satisfiability (SAT)-based attacks
  - SAT attack (see right side)
  - Approximate SAT.
  - Satisfiability Modulo Theory (SMT)-based attack
  - Iteratively prunes out wrong keys
  - Guarantees to find the correct key

Structure-based attacks

- Signal probability skew (SPS)-based attack
- Removal attack
- Other attacks specific to a locking scheme

SAT attack details





FEARLESSLY FORWARD

Attack Results

Bench	#Inputs	#Outputs	#Gates	#Flip-Flops
DES3	236	65	3606	199
GPS-PCODE	9	1	1081	162
GPS-CACODE	9	1	265	21
AES-192	323	129	188119	9382

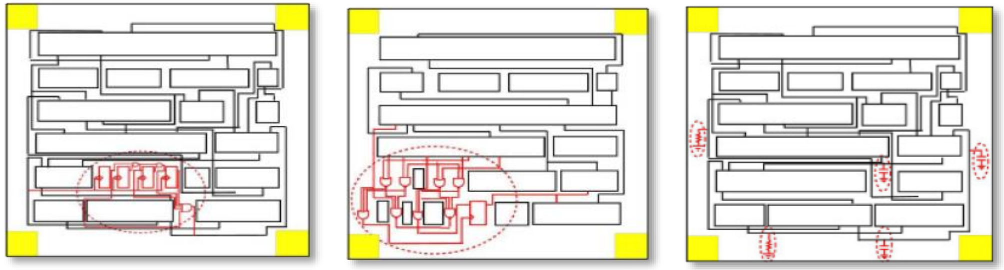
Green	Time to solve with SAT attack
Yellow	SAT completed by failed to find key
Red	SAT ran 30 days without finding key

Benchmark		DES3	GPS_PCODE	GPS_CACODE	AES-192
Seed	Key Size	Attack Time (s)			
1	16	125.6	Timeout	0.33	Timeout
	32	134.19	Timeout	0.43	Timeout
	64	217.88	Timeout	1.57	Timeout
	128	220.65	Timeout	18.78	Timeout
	256	214.16	Timeout	(224-bits) 288.37	Timeout
12	16	109.3	Timeout	0.27	Timeout
	32	127.2	Timeout	0.33	Timeout
	64	135.75	3852 (Failed)	1.71	Timeout
	128	201.9	798712 (Failed)	9.85	Timeout
	256	236.09	33664 (Failed)	(224-bits) 276.37	Timeout
123	16	121.94	Timeout	0.23	Timeout
	32	131.82	Timeout	0.31	Timeout
	64	145.82	3966 (Failed)	1.83	Timeout
	128	171.63	1750 (Failed)	10.43	Timeout
	256	201.7	Timeout	(224-bits) 211.08	Timeout

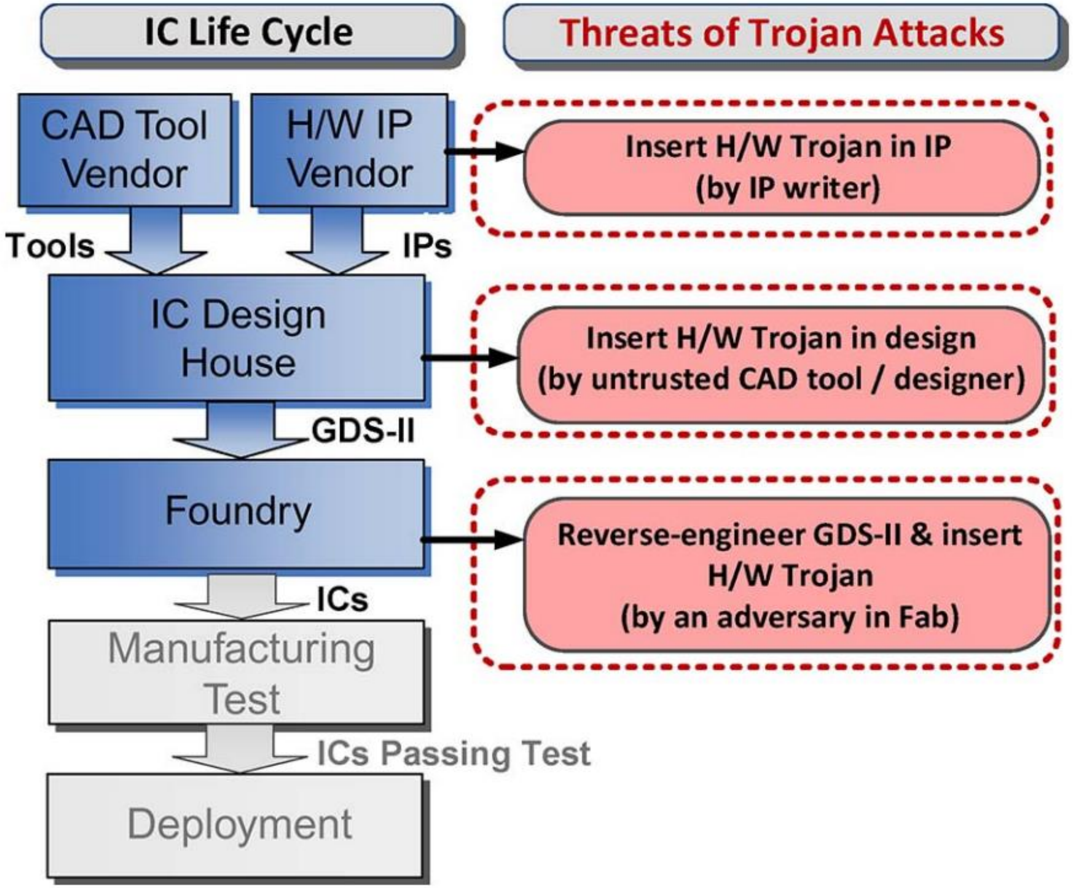
Hardware Trojan Attacks

Hardware Trojan Threat

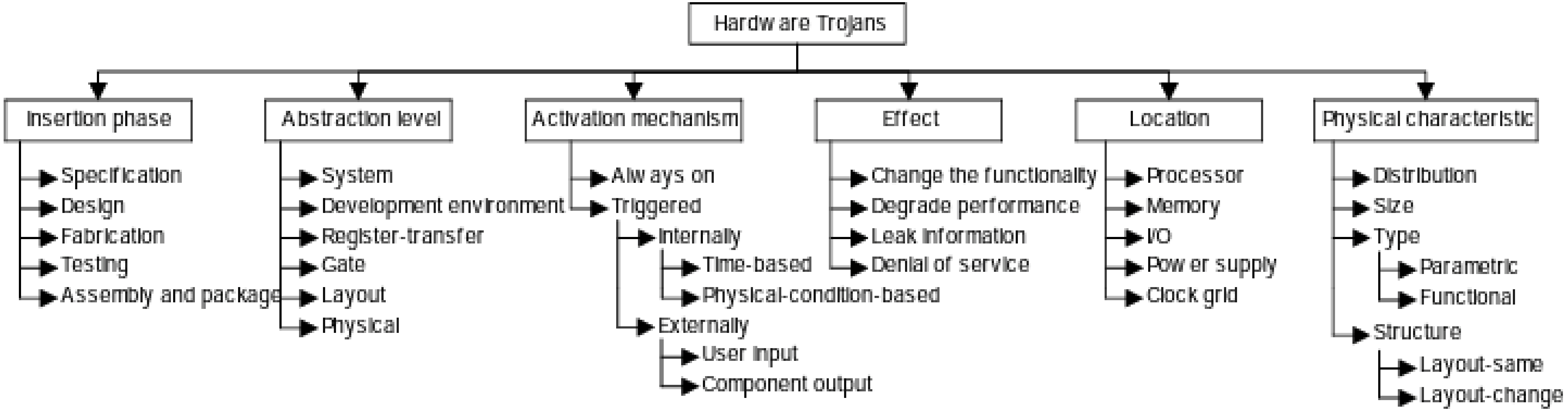
- Hardware Trojan is a malicious modification of the circuitry that can
  - Change functionality
  - Leak sensitive information
  - Denial of Service (Availability)
- Consists of
  - Trigger
  - Payload



Sequential Combinational Analog/parametric



Classification of Hardware Trojan Types

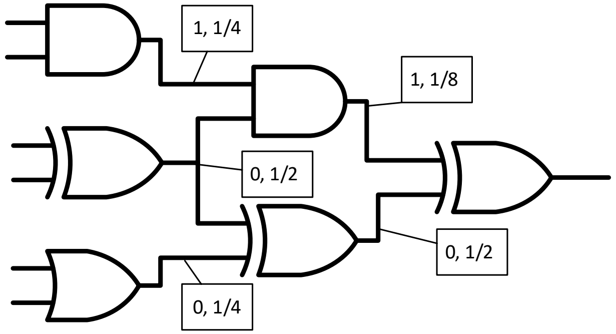


Combinational triggers	Sequential triggers	Hybrid Triggers
Rare signals	Rare branches	Combination
Rare & non-rare signals	Rare FSM states	
	Rare FSM transitions	
	Synchronous counter (increment by clock)	
	Asynchronous counter (increment by events)	
	Synchronous & asynchronous counters	
	Sequences of rare events	

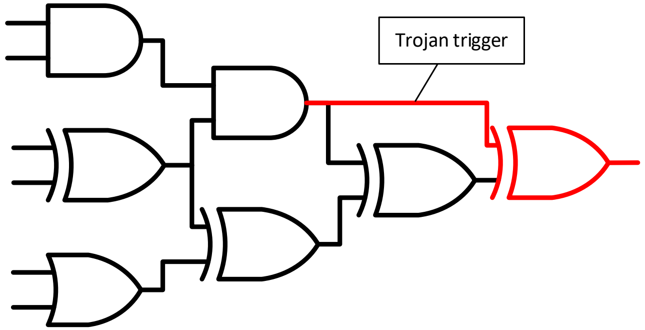
www.trust-hub.org

Examples of Triggers

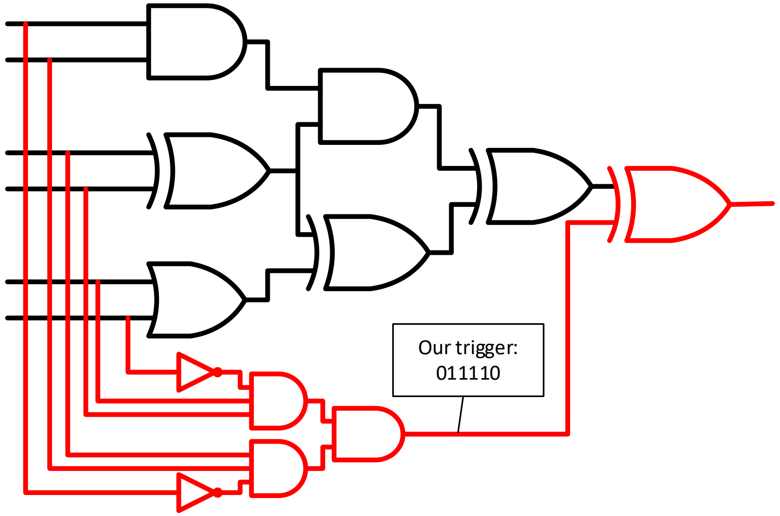
Original circuit: Annotated are the **rare value** and its probability



Conventional Trojan: using existing rare value as trigger



New Trojan Trigger: Specific pattern that does not sensitize any node's value of probability of ¼ or lower.



Based on the principles of Stripped Functionality Logic Locking

Results from our testing of a HWT Detection Tool

Rare Node Trigger HWT Detection Results

Benchmark	# Trojans	# Detected	% Detected
I2C	260	260	100%
RS Encoder	65	65	100%
Mult 32	627	627	100%

Rare + Non-Rare Node Trigger HWT Detection Results

Benchmark	# Trojans	# Detected	% Detected
I2C	100	100	100%
RS Encoder	100	84	84%
Mult 32	100	82	82%

Novel SFLL-based HWT (Artificial Rare Node) Detection Results

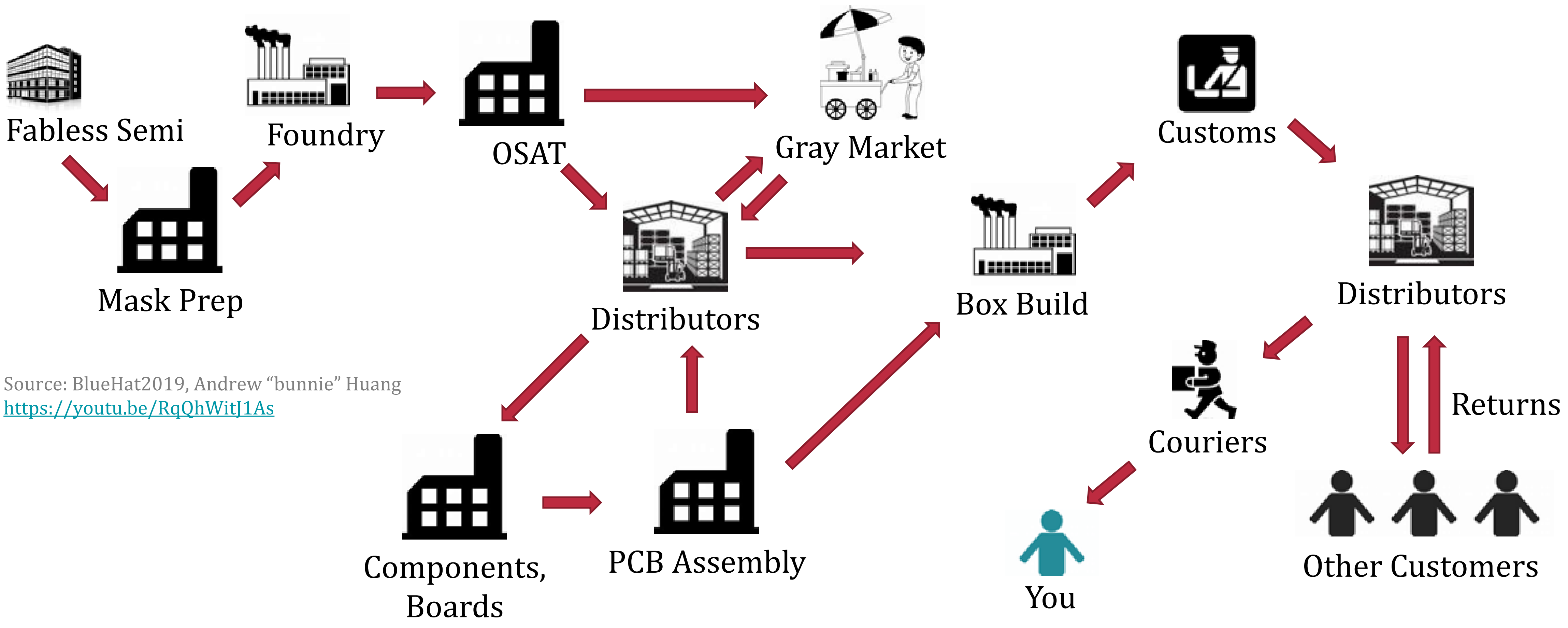
Trigger length	2	4	6	8	10	12	>=14
I2C	100%	100%	100%	100%	100%	50%	0%
RS encoder	100%	100%	100%	100%	50%	50%	0%
Mult 32	100%	100%	100%	100%	50%	50%	0%

Conclusions

1. Tool worked well for trojans that were based on the assumption that the most likely place for a Trojan insertion was in a rare node.
2. A more sophisticated Trojan became undetectable when trigger size grew large enough

Supply Chain Attacks

Semiconductor Attack Surface is Enormous

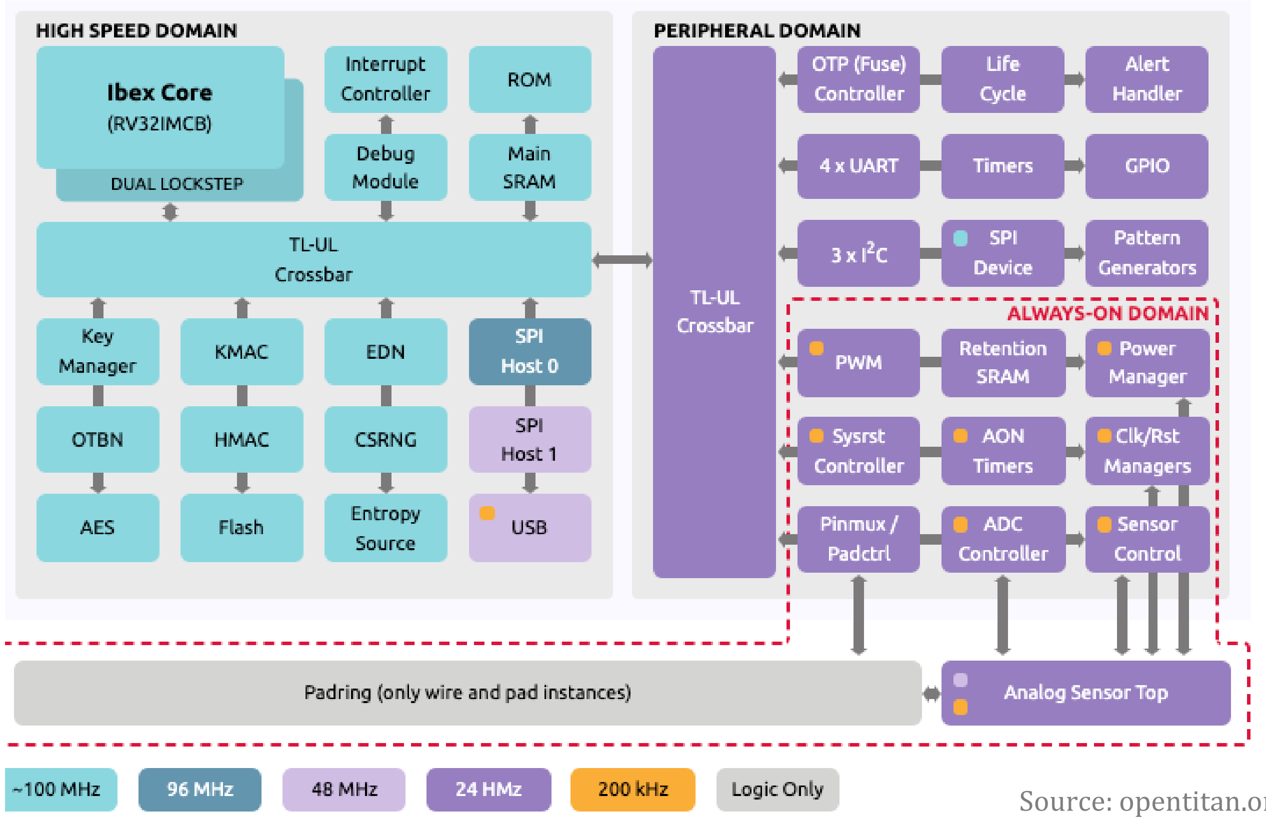


Source: BlueHat2019, Andrew "bunnie" Huang
https://youtu.be/RqQhWitJ1As

Supply Chain Attacks

- Examples of supply chain attacks
  - Counterfeit
  - Gray market
  - Overproduction
  - Recycling
  - Remarking
  - Firmware tampering
- A Root of Trust can provide
  - A means to protect identity throughout its lifecycle
  - Protection of the boot image from unauthorized code or rollback
- Core elements of such protection
  - OTP for storing unique ID
  - Lifecycle trackers
  - Cryptographic functions
  - Dynamic monitoring (HW and SW)

Open Titan is an open-source RoT



Source: opentitan.org

Design for Security Emerges as a New Skill

Seven Properties of Highly Secure Devices
1. Hardware-based Root of Trust
2. Small Trusted Computing Base
3. Defense in Depth
4. Compartmentalization
5. Certificate-based authentication
6. Renewable Security
7. Failure Reporting

Galen Hunt presentation at DARPA: https://youtu.be/XhXDkkwqgpk

Microsoft Research's Whitepaper:
https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf

Conclusion

- Hardware Security is a rapidly evolving field of expertise in semiconductors
- There has been considerable academic research, but little productization outside Root-of-Trust solutions from major suppliers
- No security is undefeatable given a well-funded and persistent attacker
- Therefore, the most practical objective is to make it as hard as possible to narrow the range of potential attackers