Permission to Use Conditions

ECE 448/548 Cyber-System Security

IC & IP Security

F. Gebali

Outline

1. Intro
2. IC/IP
3. Cloning
4. RE
5. Overproduction
6. Tampering
7. Counterfeit
8. Metering
9. Detection

Introduction

Modern IC Features

1. ICs are now very complex with urgent time-to-market
2. ICs outsource design: incorporate 3PIP
3. ICs outsource fabrication: use fab house (horizontal business model)
4. ICs outsource testing: use JTAG port
5. Integration of 5G, AI & IoT create value and motivation for attackers
6. Processors will be the ‘T’ in IoT
7. Attack surface: DoS, data theft, tampering, etc.

Ways of Compromising IC Authenticity

1. Reverse Engineering (RE) to steal intellectual property
2. Overproduction of the system to privately sell more ICs
3. Cloning replicates IC and benefit attacker
4. Counterfeiting by a competitor to sell defective or obsolete ICs
5. Tampering to alter design to leak information or DoS

Attacks on ICs

1. Unintentional design errors reduces security
2. Trojan insertion in IPs to leak data, modify function or DoS
3. Spoofing to replace original design description with a fake one to help attacker
4. Side-Channel Attacks (SCA) leaks information during encryption/decryption exposes the secret key. Also can inject faults to expose vulnerabilities
5. Reverse engineering to understand functionality and steal IP

Security of IoT

1. Security of data centre all the way down to edge devices
2. Workloads moving to the edge
3. Security at edge requires hardware root-of-trust (HRoT)
4. Security at each layer of communication stack

Defining Terms: Root of Trust (RoT)

Definition

A tursted software component to perform critical security operations and protect secret keys.

Defining Terms: Hardware Root of Trust (HRoT)

Definition

A tursted hardware component to perform critical security operations and protect secret keys.

Security of IoT/5G

1. Adversary will gain access to device eventually
2. Attacks include: RE, SCA, Fault Injection
3. HRoT (authentication + tamper proof) is a must in all devices
4. RoT integrated into application core or programmable processor

IP Types

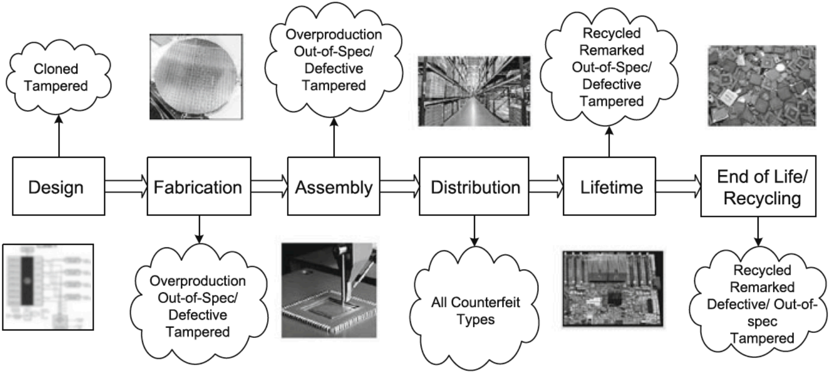
1. Soft IP: RTL code to be compiled
2. Firm IP: Netlist or gate-level description
3. Hard IP: Physical layout files as EDIF (deprecated), GDS/GDS-II or OASIS

Third Party IP (3PIP) Types: Horizontal Design Model

1. Digital IP (processors, GPU, DSP, encryption)
2. Mixed-signal IP (I/O, ADC, DAC)
3. Infrastructure IP (JTAG, test, debug, verification)

IC/IP Vulnerabilities & Attacks

ICs Supply Chain & Potential Attacks [1]



Cloned
Tampered

Overproduction
Out-of-Spec/
Defective
Tampered

Recycled
Remarked
Out-of-Spec/
Defective
Tampered

Design

Fabrication

Assembly

Distribution

Lifetime

End of Life/
Recycling

Overproduction
Out-of-Spec/
Defective
Tampered

All Counterfeit
Types

Recycled
Remarked
Defective/ Out-of-spec
Tampered

IC Lifecycle Attacks

1. Design: IP/Netlist theft
2. Mask: Theft
3. Wafer: Overproduction
4. Packaged IC: Device theft
5. Testing Phase: Discarded device reuse
6. IC Seller: Counterfeit and relabeled devices
7. Chip Salvage: Refurbishing, repackaging

Attacks on ICs

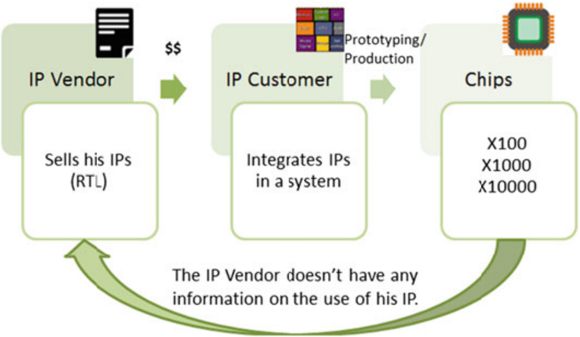
1. Hardware Trojan insertion during design or fabrication
2. Piracy Steal IP
3. Cloning 3PIP Piracy & reuse
4. Overproduction: Loss of revenue
5. Reverse engineering (RE)
6. Counterfeit ICs: Recycling old ICs & out-of-spec/obsolete ICs
7. Tampering: Inserting Trojans or extra functionality

IP Definition

1. Soft IP: RTL code to be compiled
2. Firm IP: gate-level description as Netlist
3. Hard IP: GDS/GDS-II layout file

Cloning & Over Production

IP Vulnerability: IP Piracy: Cloning & Over production [2]



1. Design house buys then clones IP
2. Design house sells GDS-II file as its own hard IP
3. Fab house can fabricate extra IC copies for private sale

Reverse Engineering or IP Piracy

Reverse Engineering (RE) or IP Piracy Approaches

1. Observe functionality
2. De-layer the IC: chemical, mechanical, X-ray
3. Extract FPGA binaries from memories

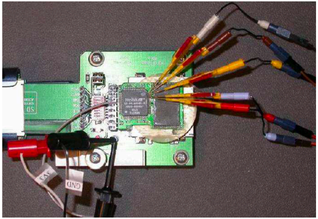
IP Vulnerability: Reverse Engineering (RE)

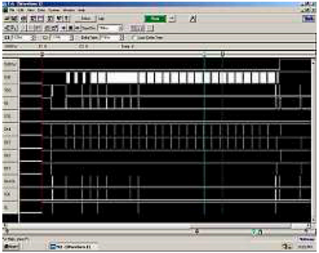
1. RE requires resources and skill
2. Functional analysis
3. Attacker could infer the gate-level netlist
4. Attacker extract circuit from the layers of the IC by etching

Reverse Engineering

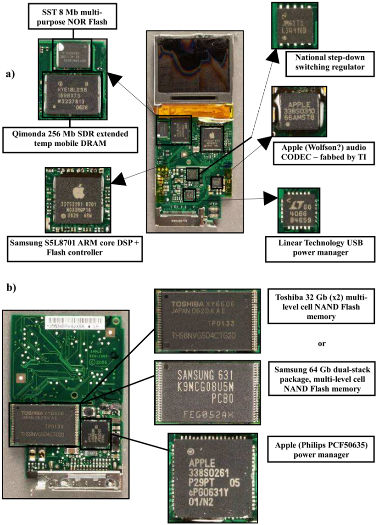
1. Depackage
2. Dissecetion
3. Take pictures
4. Cell recognition & circuit extraction
5. Schematic generation

Reverse Engineering: Functional Analysis [3]

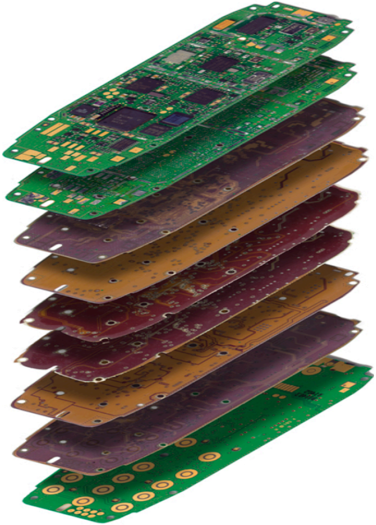




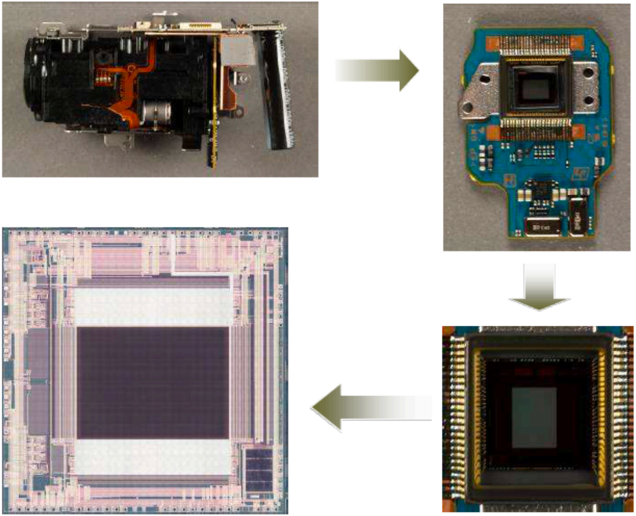
Reverse Engineering: Teardown of Apple 8 GB iPod Nano [3]


a)
SST 8 Mb multi-purpose NOR Flash
HYE18L256
169BX75
W3337813
0628
Qimonda 256 Mb SDR extended temp mobile DRAM
337S3291 8701
N033RQP16
0629 ARM
Samsung S5L8701 ARM core DSP + Flash controller
JM62TS
L3441OB
National step-down switching regulator
APPLE
338S0310
66AMST8
Apple (Wolfson?) audio CODEC – fabbed by TI
4066
84659
Linear Technology USB power manager
b)
TOSHIBA XY6606
JAPAN 0629 KAE
TP0133
TH58NVG5D4CTG20
Toshiba 32 Gb (x2) multi-level cell NAND Flash memory
or
SAMSUNG 631
K9MCG08U5M
PCB0
FEG052AH
Samsung 64 Gb dual-stack package, multi-level cell NAND Flash memory
APPLE
338S0261
P29PT 05
cPG0631Y
01/N2
Apple (Philips PCF50635) power manager

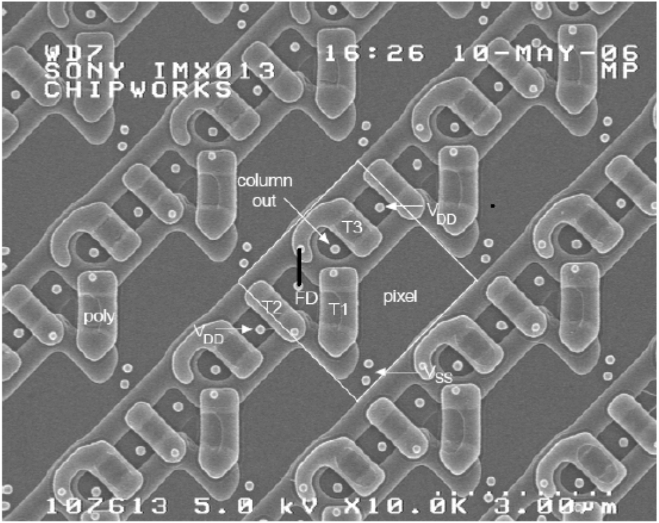
Reverse Engineering: Teardown of Cell Phone PCB Layers [3]



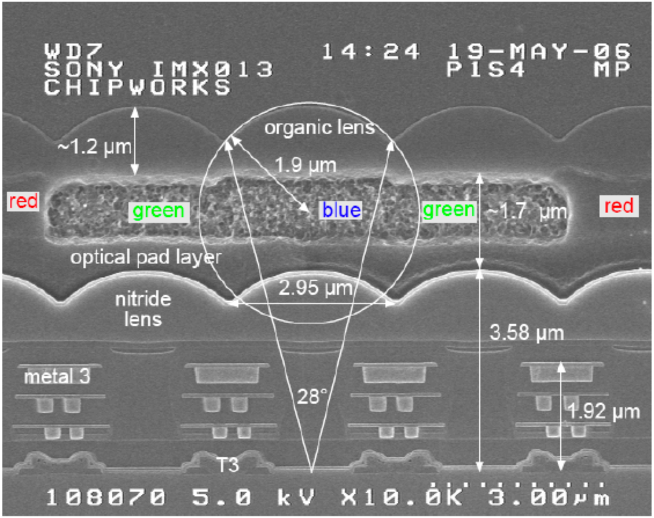
Reverse Engineering: Teardown of Camera [3]



Reverse Engineering: Teardown of Camera: SEM Top View



Reverse Engineering: Teardown of Camera: SEM Cross-Section



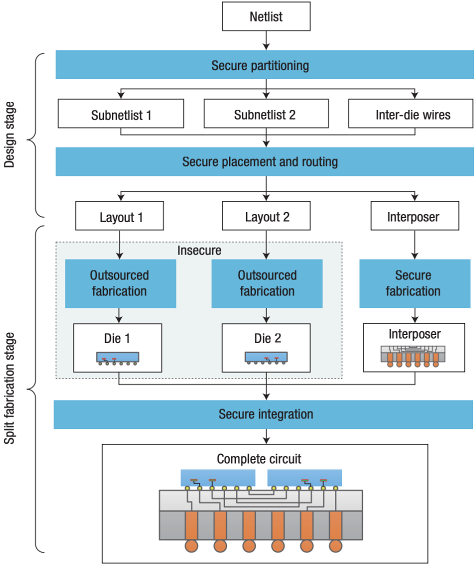
RE Countermeasures [6]

1. 2.5D Manufacture
2. Tamper resistance (prevent RE)
3. Metering or Hardware locks [4]
4. Measure Aging of IC
5. Design obfuscation (thwart RE)
6. Build physical unclonable function (PUF) [5]
7. Integrated circuit authentication [1]
8. Hardware locks [4]
9. ⋮

Security-Aware 2.5D Split Fabrication [7]

1. Split the design is split:
   1. Two or more silicon cores
   2. Place the dies onto a silicon interposer
2. Outsource the silicon cores to untrusted foundries
3. Fabricate the interposer in trusted foundry
4. Some of the wiring is hidden on the interposer silicon
5. Final fabrication is in trusted foundry

2.5D Design Flow



Overproduction

Overproduction

1. Outsourcing fab allows the fab house to produce more ICs and sell privately
2. This short changes the design house

Counterfeiting: Out-of-Spec/Defective/Rejected ICs

1. Defective ICs are sold as good ICs
2. Rejected ICs are either stolen or sold by foundry

Dangers of Using Obsolete Devices

1. Aging changes IC performance parameters
2. Aging reduces IC reliability
3. Changes in MOS threshold voltage leads to increased gate delays
4. Ring oscillator can be used to measure delay variations & aging

Counterfeiting: Cloned ICs

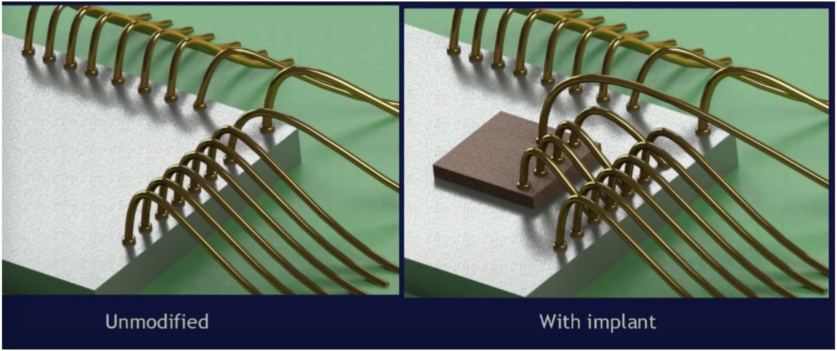
Definition

Unauthorized production of an IC without having the legal IP

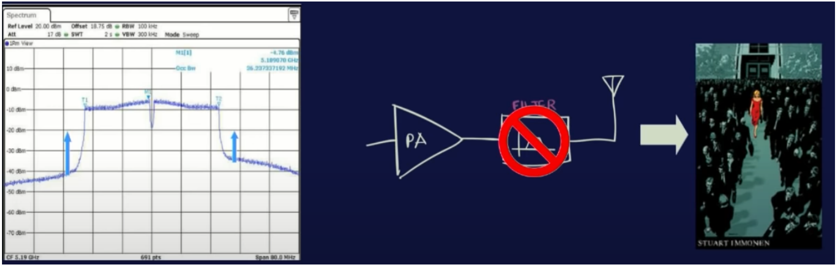
1. Similar to overproduced ICs that use legal IP for the product
2. Clone through reverse engineering (RE)
3. Clone through stolen IPs

IC Tampering

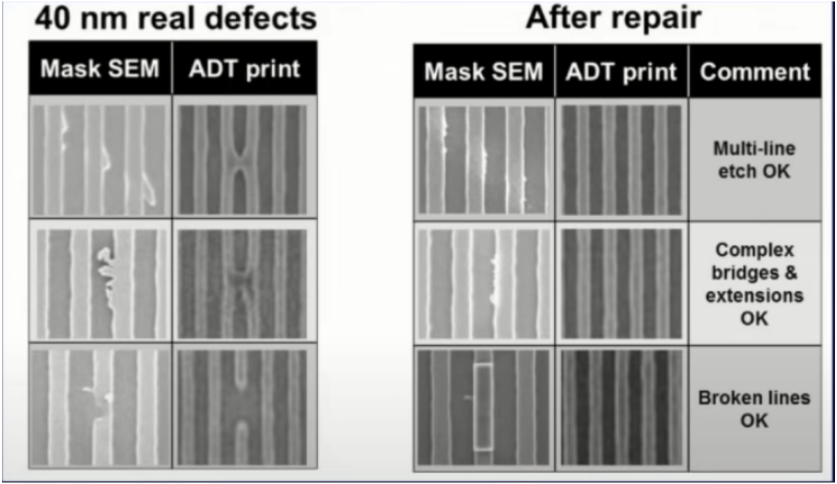
Tampering Example: Insert Bad IC Inside another IC



Tampering Example: Insert Bad IC Inside another IC



Tampering Example: IC Mask Editing (Good and Bad)



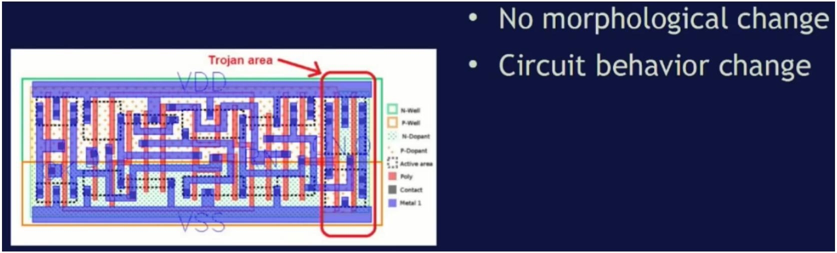
40 nm real defects

Mask SEM	ADT print

After repair

Mask SEM	ADT print	Comment
		Multi-line etch OK
		Complex bridges & extensions OK
		Broken lines OK

Tampering Example: IC Doping Modification at Mask Level

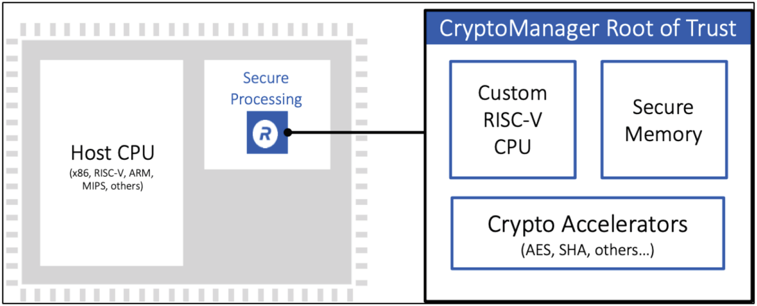


- No morphological change
- Circuit behavior change

Tampering Objectives

1. Steal information
2. Denial of service (DoS)
3. Defeat usage limitations policies
4. Reverse engineer IC

Countermeasures: Tamper Resistance



This is discussed in Secure Processor Design lectures.

IC Counterfeiting

Counterfeit ICs

1. Counterfeit chips is used more often nowadays
2. Counterfeit ICs include: analog ICs, microporcessors, memory, and FPGAs
3. ICs are found in all electronic products and using counterfeiting is a way to reduce costs or facilitate later attacks
4. Detection and avoidance are current areas of research

Dangers of Using Counterfeit Chips

1. Functionality: non-conforming specifications
2. Reliability: bad solder joints in counterfeit PCBs
3. Reliability: bad bonding of die to padframe
4. Performance: out-of-spec parameters

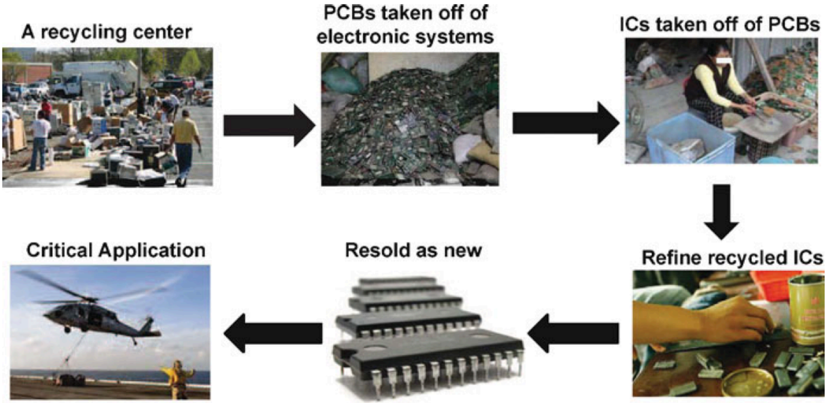
The Different Types of Counterfeit Chips

1. Recycled
2. Cloned
3. Re-labeled
4. Unauthorized ICs: overproduced
5. Out-of-spec, defective, rejected, or obsolete
6. Remarked labels
7. Tampered or altered

Counterfeiting: Recycled ICs

1. Extracted ICs from PCB could reduce functionality
2. Aged ICs have aging effects (reliability, parameter shift, $\cdots$

Counterfeit ICs: Recycling Old ICs



Counterfeiting: Re-labeled ICs

Definition

Removal of the labels on the package (or die) and labeling with forged information

1. Re-labeling to increase IC value: 1 GHz μP claims to be a 1.2 GHz μP
2. Re-label new commercial IC as military grade
3. Re-label old IC as new IC

Reality about IC Counterfeits

1. 1,000,000 counterfeit components in US military systems
2. 70% of these devices came from abroad
3. 30% of these devices traced back to potential adversaries
4. $1.69 B counterfeit electronics in circulation
5. Commerce is targeted by bad companies
6. Military is targeted by adversarial countries

Counterfeiting Physical Detection

1. Visual inspection
2. X-ray inspection
3. Unpackeging and high-resolution inspection
4. Electrical inspection: Power, leakage, delay
5. Functional verificaton

Metering
Digital Rights Management (DRM)

IC Metering Definition

Definition

IC metering is a set of security protocols that enable the design house to achieve post-fabrication control over their ICs. These protocols could be passive or active.

DRM

There is similarity between hardware DRM and software license management (SLM)

DRM provides a solution to IC/IP piracy by initially locking IC/IP

1. Date methods
2. Usage time methods
3. One-time activation code (controller, flip-flops, etc)
4. Activate each time IC/IP is used (related to DoS Trojans)
5. Each IC/IP should have a unique unclonable ID

Active vs. Passive Metering

1. Passive metering gives each IC a unique ID using a stored serial number or incorporating a PUF to passively track it
2. Active metering allows the designer to lock/unlock the device
3. Active or passive metering rely on a unique ID for each device
4. An unclonable ID is to use PUFs and relies on authentication before unlocking the IC
5. Using PUFs requires trusted foundry

IC Activation

1. Device use cryptographic protocol to activate
2. Clones could not be activated
3. Must contact IP vendor or design house to get permission
4. Use encryption to:
    1. Activate datapath
    2. Antifuse on chip
    3. FPGA bitstream encryption

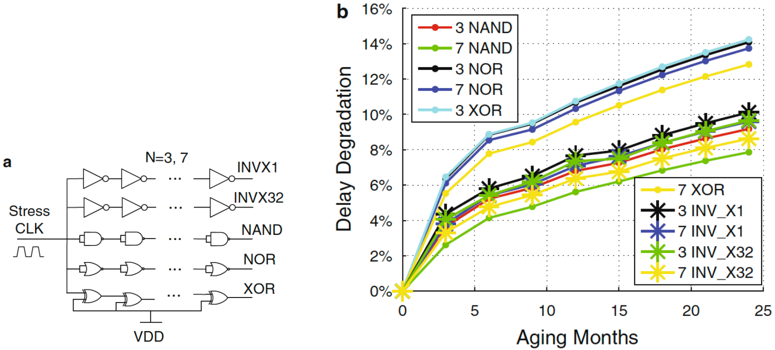
Examples of Counterfeit Chips

1. Counterfeit IC is one that is not genuine
2. Unauthorized copy
3. Does not conform to original specs, defective, or recycled but labeled as new
4. Not produced by original fab house
5. Has incorrect label or documentation

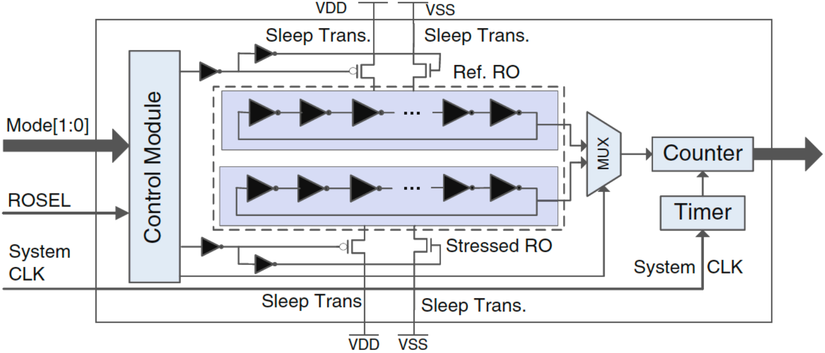
Why Chips Age [1]

1. MOS threshold voltage changes with time and this degrades performance
2. Best to use ring oscillators with high high thresholds to speed aging in these circuits
3. Must measure frequency changes in RO to determine age of IC
4. Must also distinguish between aging and normal inter-chip random process variations (RPV)

Countermeasures: Measure Aging Using Ring Oscillator [1]



Countermeasures: Measure Aging Using Ring Oscillator (RO) [1]



1. Frequency of RO is used to measure aging
2. Sleep transistors isolate reference RO from operation
3. Two ROs closely placed to eliminate process variations

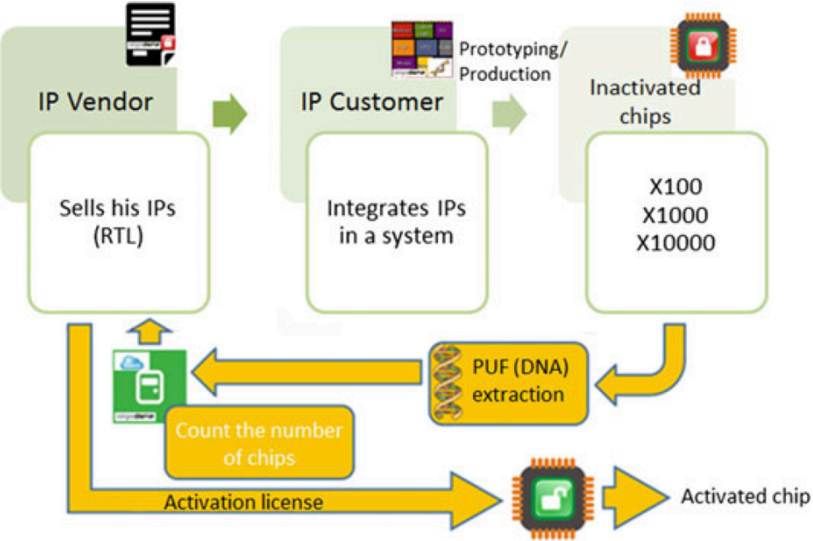
I/O Locks: Using D-FF with Enable

1. All I/O should be obtained through a D-type FF
2. All D-FF must have an enable signal
3. When device is authenticated, enable signal is high
4. Normal mode is when enable signal is high
5. Locked mode is when enable signal is low

Processor Lock: Program Counter

1. All SoC have soft- or hard processors
2. Processor is disabled through program counter (instruction pointer)
3. Freezing this counter disables the processor

DRM: PUF-based Smart Lock [4]



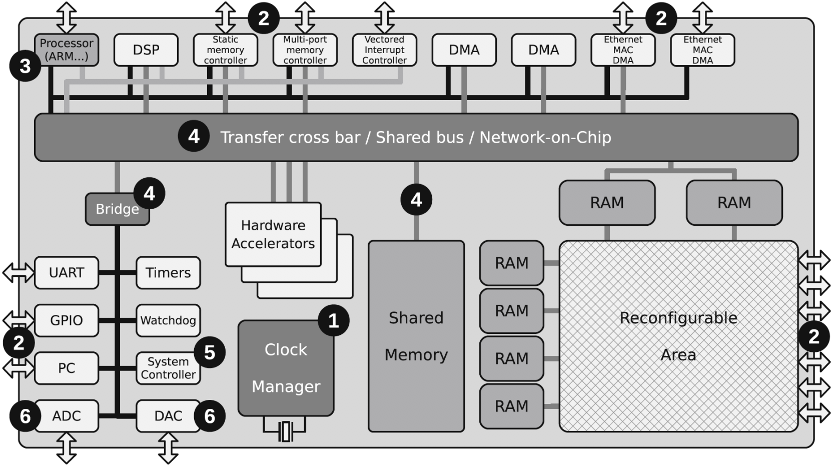
Considerations of PUF-based Smart Lock

1. The PUF response is only known after the IC is actually manufactured

2. The fab house is the first entity able to extract the PUF response. Fab house must be trusted.

3. IP vendor might be able to implement the PUF as a software entity. Is it even possible? Is it secure?

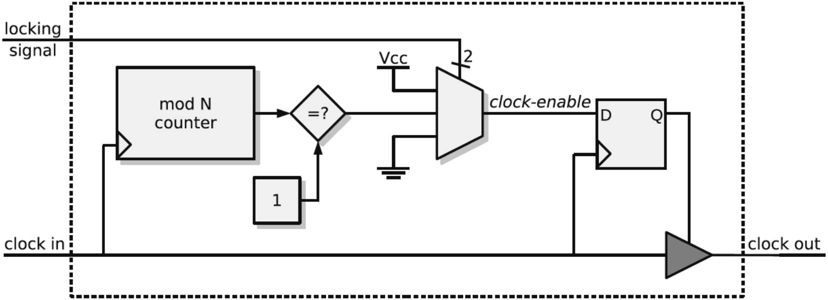
Countermeasures: Metering via Hardware Locks for SoC [4]



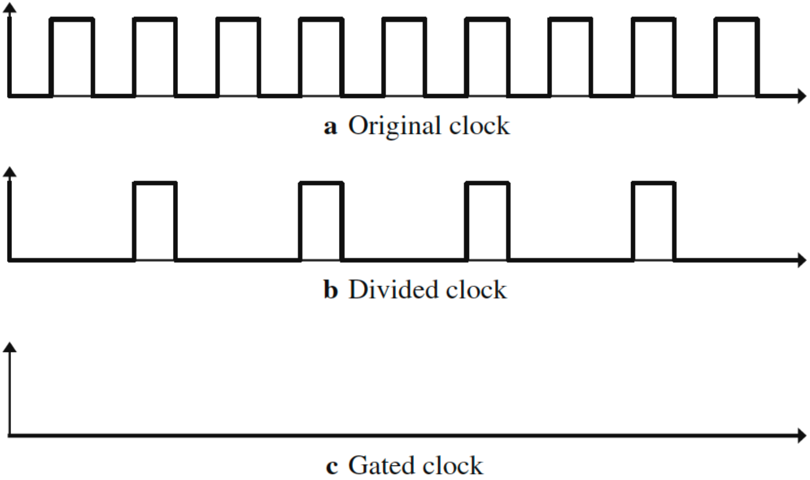
Components the could be used as Hardware Locks

1. The clock manager
2. The inputs/outputs,
3. The processor,
4. The interconnection buses,
5. The system controller,
6. The analogue components.

DRM: Clock Lock Through Gating [4]



DRM: Clock Lock Through Gating [4]



a Original clock

b Divided clock

c Gated clock

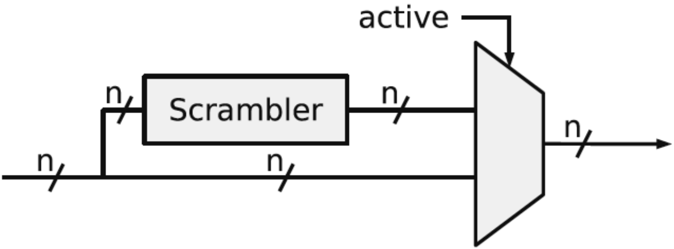
DRM: I/O Locks Using D-FF with Enable

1. All I/O signals normally go through D-type FFs
2. All D-FF must have an enable signal
3. When device is authenticated, enable signal is high
4. Normal mode is when enable signal is high
5. Locked mode is when enable signal is low

DRM: Processor Lock Through Program Counter

1. All processors have a program counter (PC)
2. PC contains address of instruction currently executed
3. Fixing PC content effectively halts the processor
4. State of PC can by dynamically changed to allow for normal, halt and evaluate modes

DRM: Locking Buses [4]



1. Can scramble the data bus lines
2. Can scramble the address buss lines

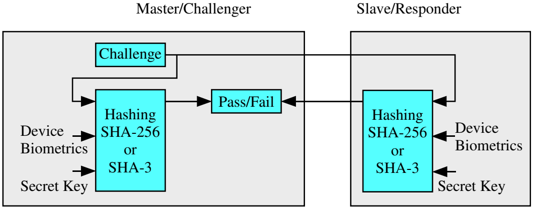
Counterfeit Detection Methods Taxonomy

Counterfeit Detection: Authentication Methods

1. Physical metrics
2. Using challenge and valid response using a secret key
3. Challenged device constructs response using secret key
4. Key could be shared (symmetric) or not shared (public key)

Counterfeit Detection: Authentication with Symmetric Key Cryptography

1. Challenger issues a random challenge
2. Hashing could be SHA-256, SHA-3, or SHA-3 light, etc.
3. Digital signature is used for authentication
4. Key is hard-coded
5. Challenge could include device ID and biometrics



Countermeasures: Design Obfuscation

1. Turn a simple algorithm to a very complex one
2. Ad hoc with no universal techniques
3. Applies to hardware as well as software

Countermeasures: Design Obfuscation Examples

1. Complicated wire routing
2. Scatter connected gates over the chip
3. Add undocumented states and commands

[1] M. Tehranipoor, H. Salmani, and X. Zhang, *Integrated Circuit Authentication: Hardware Trojans and Counterfeit Detection*. Springer, 2014.

[2] L. Torres, P. Benoit, J. Rampon, R. Perillat, D. Spring, G. Paul, S. Bonniol, and L. Bossuet, “Digital right management for IP protection,” in *Foundations of Hardware IP Protection*, L. Bossuet and L. Torres, Eds. Springer, 2017.

[3] R. Torrance and D. James, “The state-of-the-art in ic reverse engineering,” in *International Workshop on Cryptographic Hardware and Embedded Systems: Cryptographic Hardware and Embedded Systems*, 2009, pp. 363–381.

[4] B. Colombier, L. Bossuet, and D. Hély, “Turning electronic circuits features into on-chip locks,” in *Foundations of Hardware IP Protection*. springer, 2017.

[5] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in *Design Automation Conference*, 2007, pp. 9–14.

[6] S. Guilley, J.-L. Danger, R. Nguyen, and P. Nguyen, “System-level methods to prevent reverse-engineering, cloning, and trojan insertion,” in *Communications in Computer and Information Science*, S. Dua, A. Gangopadhyay, P. Thulasiraman, U. Straccia, M. A. Shepherd, and B. Stein, Eds. Springer, 2012, vol. 285, pp. 433–438.

[7] Y. Xie, C. Bao, and A. Srivastava, “Security-aware 2.5D integrated circuit design flow against hardware IP piracy,” *IEEE Computer*, pp. 62–71, May 2017.