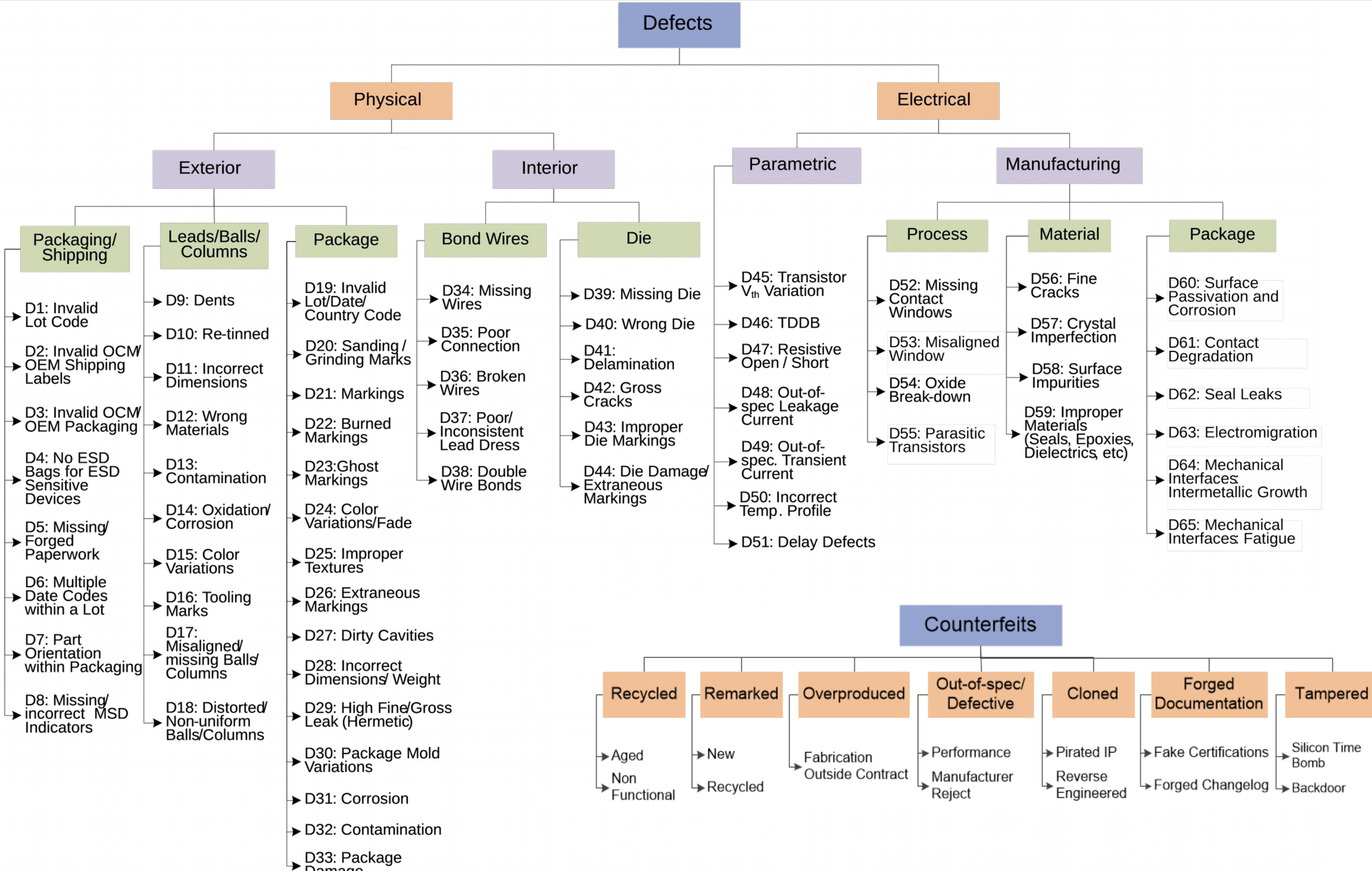
ECE 459/559
Secure & Trustworthy Computer Hardware Design

Counterfeit Mitigation

Garrett S. Rose
Spring 2017

THE UNIVERSITY OF TENNESSEE KNOXVILLE

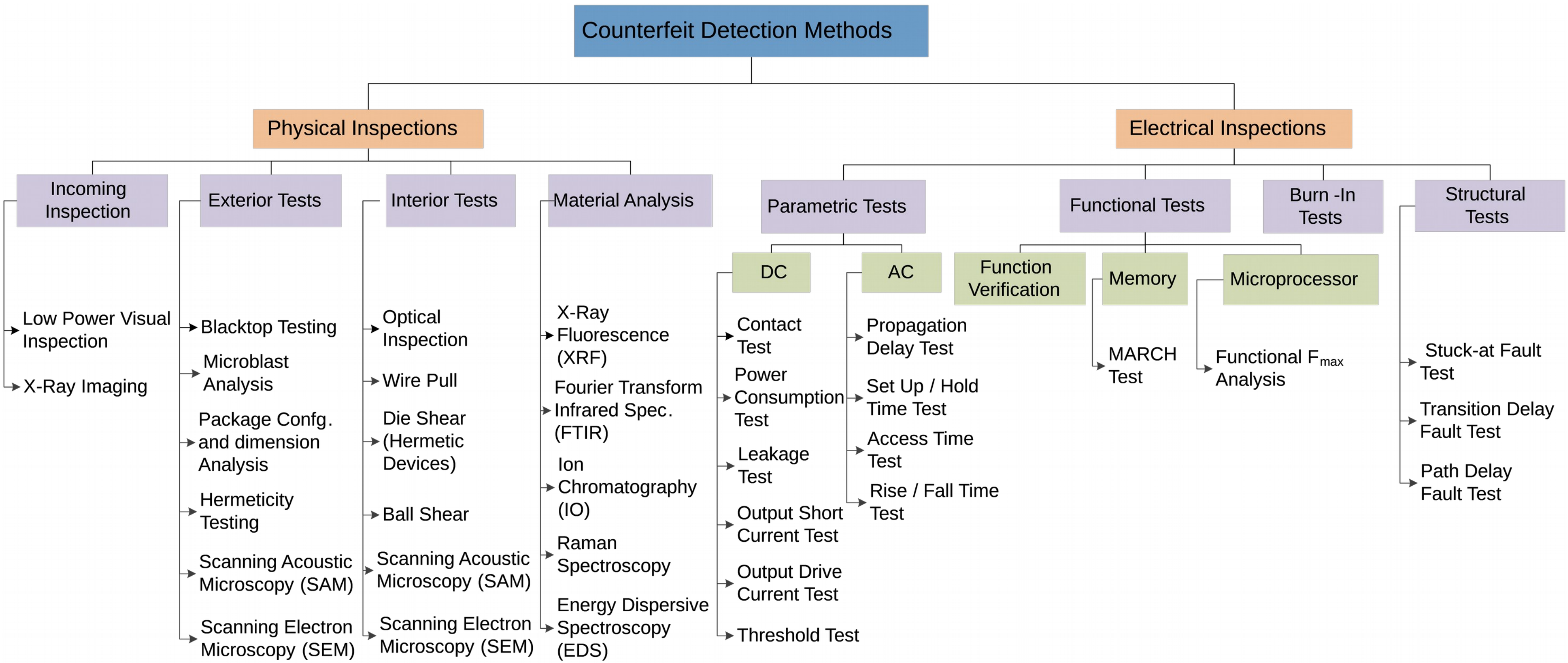
Counterfeit Defect Taxonomy



Testing for Defects

THE UNIVERSITY OF
TENNESSEE
KNOXVILLE

Detection Method Taxonomy



External Visual Inspection (EVI)

- EVI:
  - All devices optically examined at suitable magnification (3X to 100X)
  - Portion of inspection (sampling) performed at 40X or higher
  - IDEA-STD-1010-A good reference
- Detailed EVI Inspection:
  - Sample size of 119 devices selected
  - Normally 116/c samples inspected for 90% confidence and at most 2% failures
  - Additional 3 samples used for marking permanency, lead finish (XRF), and Delid Physical Analysis (DPA)

Burned markings from low quality laser

Verification of:
- Date & Lot Codes
- Low Power Microscopy
- High Power Microscopy
- OEM Shipping Labels
- Lead Quality
- Dimensions & Weight
- Marking Quality

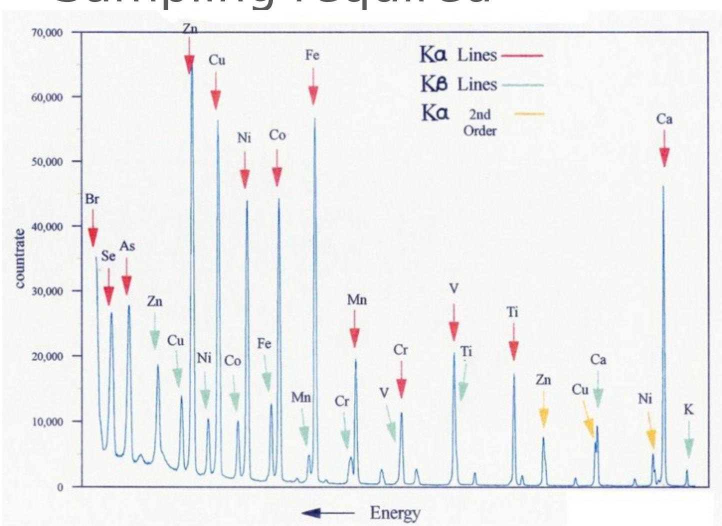
THE UNIVERSITY OF TENNESSEE KNOXVILLE

More on EVI

- Test for Remarking and Resurfacing
  - First set of tests focus on part marking, is a resistance to solvents test
  - Markings should not smear or be removed by the solution
- Test for Resurfacing
  - Uses same 3 devices, consists of three separate chemical tests
    - Acetone Test
    - 1-Methyl, 2-Pyrrolidinone Test
    - Dynasolve 750 Test
  - Looks for indicators of package resurfacing and recoating
  - 3 devices that pass this inspection then undergo Delid Physical Analysis Inspection

X-Ray Fluorescence (XRF) Spectroscopy

- Tool for material composition detection
- Can be a handheld instrument or a full lab system
- Can be on external surfaces or de-lidded/de-capsulated
- Non-destructive
  - Destructive for internal material composition (e.g., wire bond, passivation, and metalization)
- Sampling required



More on XRF

- Lead finish examination
  - Performed on the 3 sample devices
  - Examined for remarking and resurfacing
  - Verify that lead finish / solder ball and column composition matches device specifications and/or datasheet
- Plating material(s) identification
  - Verify plating layer thicknesses, presence of barrier materials, and possibly the base material

Delid Physical Analysis

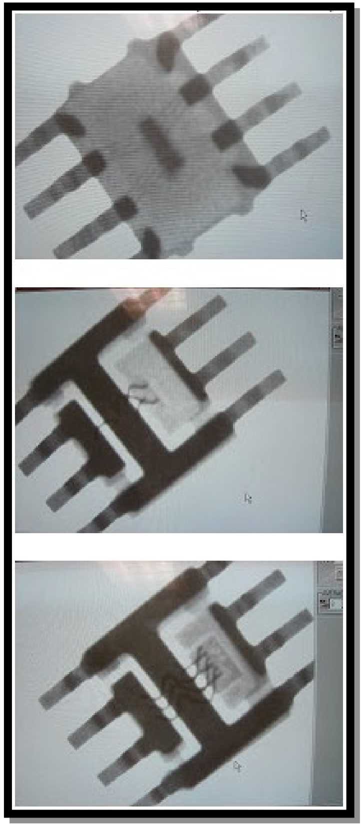
- The inspection:
  - Component's internal structure
  - Top surface of a microelectronic die
  - Metalization traces of a thin-film resistor
- Apparatus & Equipment:
  - Chemical Decapsulation Process
    - Use of hazardous chemicals (Nitric acid and sulfuric acid)
  - Mechanical Disassembly Tools
    - Includes cross-section tables and associated epoxy mounting material, fine-tipped picks, x-acto blades, etc.
  - Radiographic Tool
  - Metallurgical Microscopes and Photodocumentation Equipment
  - Scanning Electron Microscope (SEM), Energy Dispersive X-ray (EDX)

Risk Level Inspection Test

	Critical Risk	High Risk	Moderate Risk	Low Risk
	4	3	2	1
Optically Inspect/Photo document	X	X	X	X
Wire Pull	X	X	X	(optional)
Die Shear (hermetic)	X	X	(optional)	(optional)
Ball Shear	X	X	(optional)	(optional)
SEM Inspection	X	(optional)	(optional)	(optional)
Perform EDX	X	(optional)	(optional)	(optional)
Delayer/Inspect Metalization	X	(optional)	(optional)	(optional)
Glassivation Layer Integrity Testing	X	(optional)	(optional)	(optional)

X-Ray Inspection

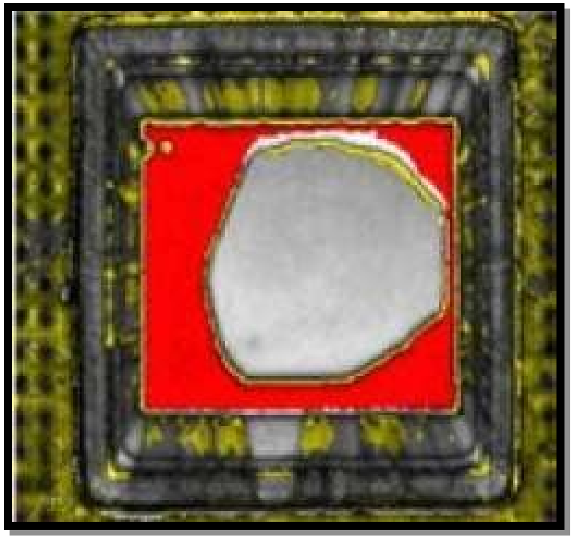
- Determines:
  - If the package contains a die
  - Consistent size/shape of the die
  - Consistent internal construction
  - If the die has all wire bonds attached
  - Exact die and bond wire location
    - To avoid damage during decapsulation



“The value of X-ray is increased when there is a known good OCM device available for comparison of internal details.”
– CCAP-101 Certified Document Rev D

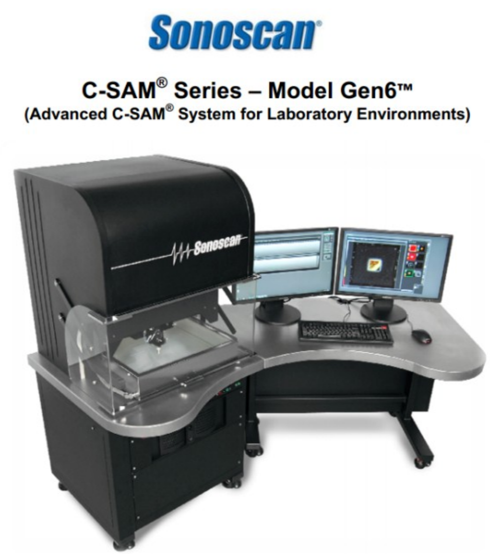
Scanning Acoustic Microscopy

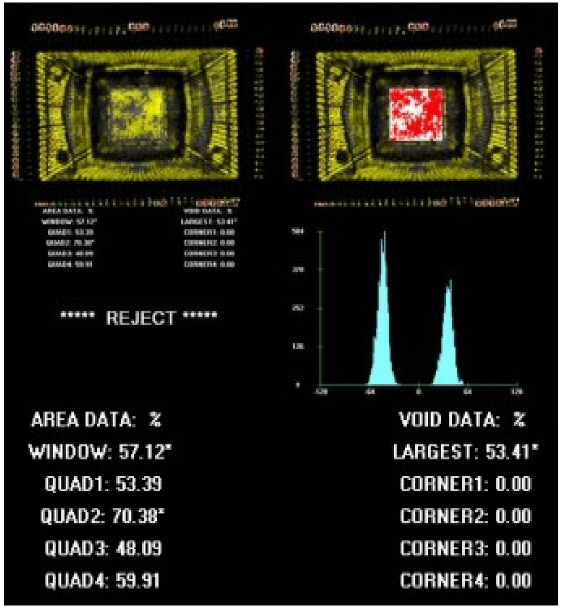
- Acoustic is non-invasive
  - Reveal cracks, voids, and delamination
  - Non-destructive die inspection
  - Uses de-ionized water or IPA as medium



MuAnalysis *look deeper*

Red areas indicate delamination



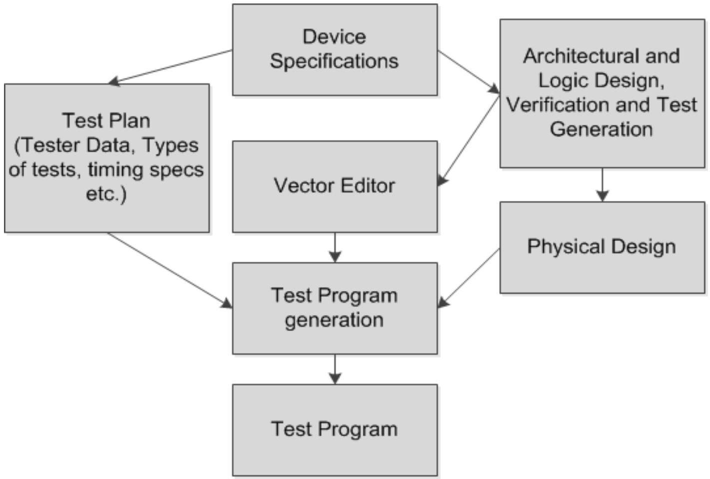


Electrical Tests

- Mainly focus on large scale integrated circuits
  - Microprocessors, memory, and programmable logic chips account for about 35% of all counterfeits
- As these are high cost parts, counterfeiter will probably put more effort in counterfeiting and detection is difficult
- No definite test methodology either electrical or physical (without destroying the chip) to achieve 100% confidence

Electrical Tests

- ATE (Automated Test Equipment)
  - Speed (clock rate of device)
  - Timing (strobe) accuracy
  - Number of I/O pins, etc.
- Test Programming
- Limitations:
  - HDL description of test module must be available
  - No definite methodology to detect counterfeit ICs



Recycled Parts: Aging

- Recycled parts are around 80% of total counterfeit parts
- Most of the defects in recycled parts are due to aging
- Aging mechanisms:
  - Negative bias temperature instability (NBTI)
    - Occurs in p-channel of MOS devices stressed with negative gate voltages and elevated temperature, due to generation of traps at Si-SiO_2 interface
  - Hot carrier injection (HCI)
    - Occurs in NMOS devices causes by trapped interface charge at Si-SiO2 surface near drain end during switching
  - Time-dependent dielectric breakdown (TDDB)
    - Carrier injection with high electric field leads to gradual degradation of oxide properties, eventual destruction of dielectric
  - Electromigration
    - Mass transport of metallic ions stressed at high current densities

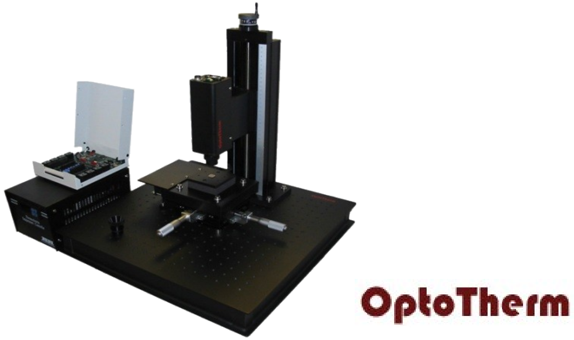
Parametric Test

- DC Parametric Test
  - Contact test
  - Power consumption test
  - Leakage test
  - Output short current test
  - Output drive current test
  - Threshold test
- AC Parametric Test
  - Propagation delay test
  - Setup/hold time test
  - Access time test
  - Rise and fall time test

Functional Testing

- Most efficient method for verifying functionality of a component
- Functional verification of a component
  - Determine whether individual components function as a system and produce expected response
- Memory tests
  - Read/write operations performed on memory to verify functionality – MARCH tests can be applied for counterfeit detection
- Microprocessor tests
  - Microprocessors are binned in different groups depending on maximum functional frequency (f_{max})

Temperature Cycling / Burn-In



- Test chip at extremes of operating range
- Tester ranges:
  - Military grade: -65C to 175C
  - Industrial grade: -25C to 85C
  - Commercial grade: -10C to 70C
- Burn-in:
  - Device operated at elevated temperature (stressed condition)
  - Use to find mortality failures and unexpected failures, assure reliability
  - Test methods:
    - MIL-STD-883 for integrated circuits
    - MIL-STD-750 for other discrete components
  - Very useful for weeding out commercial components marked military
  - Can remove defective component or those not designed for certain conditions

Structural Testing

- At-speed tests
  - To detect gross and spot delay defects
  - Transition delay fault test / Path delay fault test
- Stuck-at tests
  - To detect spot delay defects
- Bridging tests
  - To detect physical bridging defects

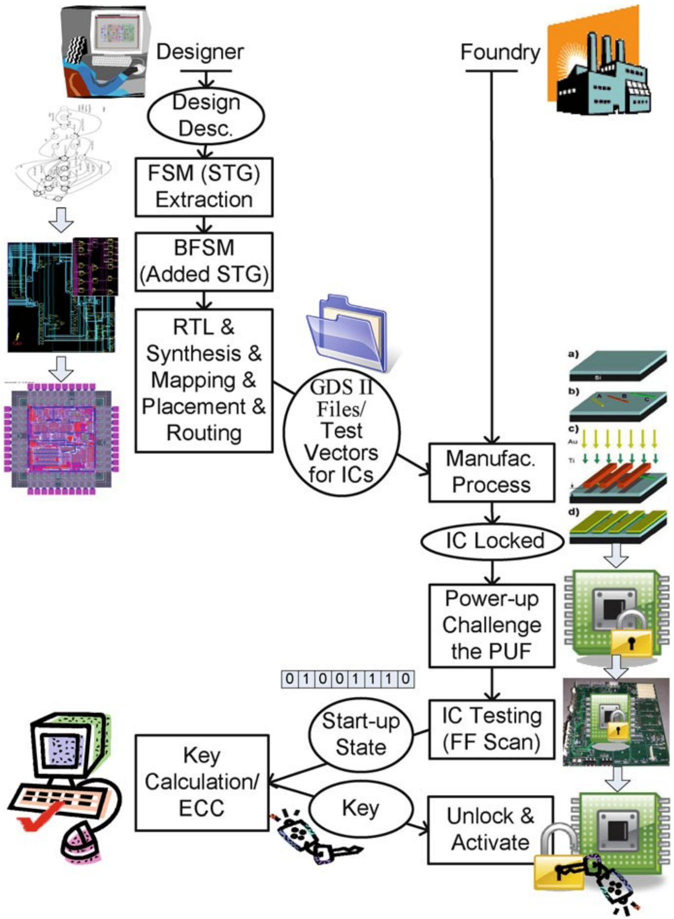
Hardware Metering

- Set of security protocols that enable design house to achieve post-fabrication control over their fabricated ICs
- Provides way to uniquely fingerprint or tag each chip and/or each chip's functionality
  - It is possible to distinguish between different chips manufactured by same mask
- First introduced in 2005
  - First instance designed to uniquely tag each IC's functionality

Hardware Metering

- Passive IC metering
  - IDs on the package
  - IDs stored in memory
    - Pentium III Processor (PSN: Processor Serial Number)
  - Unclonable identifiers
    - Generate IDs utilizing process variations
- Active IC metering
  - Uniquely and unclonably identifies each chip
  - Provides active mechanism to control, monitor, lock, or unclock the IC after fabrication

IC Enabling by Active Metering



THE UNIVERSITY OF TENNESSEE KNOXVILLE

Physical Unclonable Function (PUF)

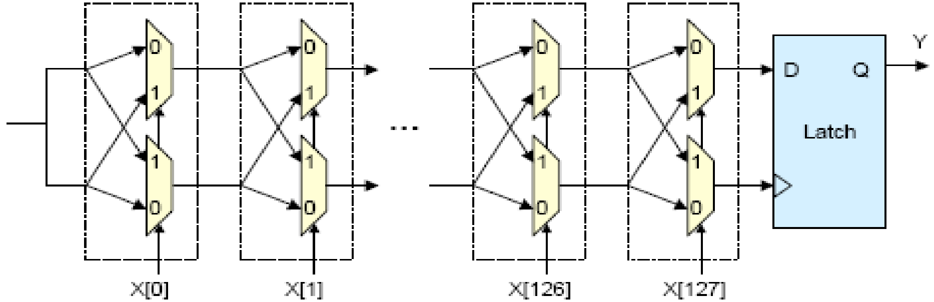
- Derive secret from complex physical characterics of IC rather than storing the secret in digital memory
- Extremely difficult to predict or extract the secret as PUF utilizes random process variations to generate the secret
- PUF generates volatile secrets (only exist in digital form when chip is powered on and running)
  - More difficult for an invasive attack (must accurately measure PUF delays while powered on)

More on the PUF

- A PUF is a function that maps a set of challenges to a set of responses based on complex physical system
- The function
  - Can only be evaluated with the actual physical system
  - Is unique for each physical system because of random process variations

PUF Examples

Arbiter PUF:



RO PUF: