Counterfeit Integrated Circuits: Threats, Detection, and Avoidance

Domenic Forte
Assistant Professor
ECE, University of Florida

Rajat Subhra Chakraborty
Associate Professor
CSE, IIT Kharagpur

Tutorial Outline

SECTION I: Impacts of Electronic Counterfeiting and Hardware IP Piracy *(20 minutes)*

SECTION II: Adversarial Models and Counterfeit Taxonomies *(15 minutes)*

---------- BREAK (*10 minutes*) ----------

SECTION III: Counterfeit Detection Approaches *(20 minutes)*

SECTION IV: Advanced / Automated Physical Inspection *(20 minutes)*

---------- BREAK (*10 minutes*) ----------

Tutorial Outline

SECTION V: Counterfeit Avoidance Approaches *(25 minutes)*

SECTION VI: Advanced Counterfeit Avoidance of COTS memories (SRAM, Flash) and FPGAs *(25 minutes)*

---------- BREAK (*10 minutes*) ----------

SECTION VII: IP Encryption and Cryptographic Flaws Uncovered in IEEE P1735 Standard; FORTIS for End-to-End Protection of IP *(30 minutes)*

SECTION VIII: Open Problems and Future Research Directions *(20 minutes)*

SECTION IX: Conclusion *(5 minutes)*

Section I: Impacts of Electronic Counterfeiting and Hardware IP Piracy

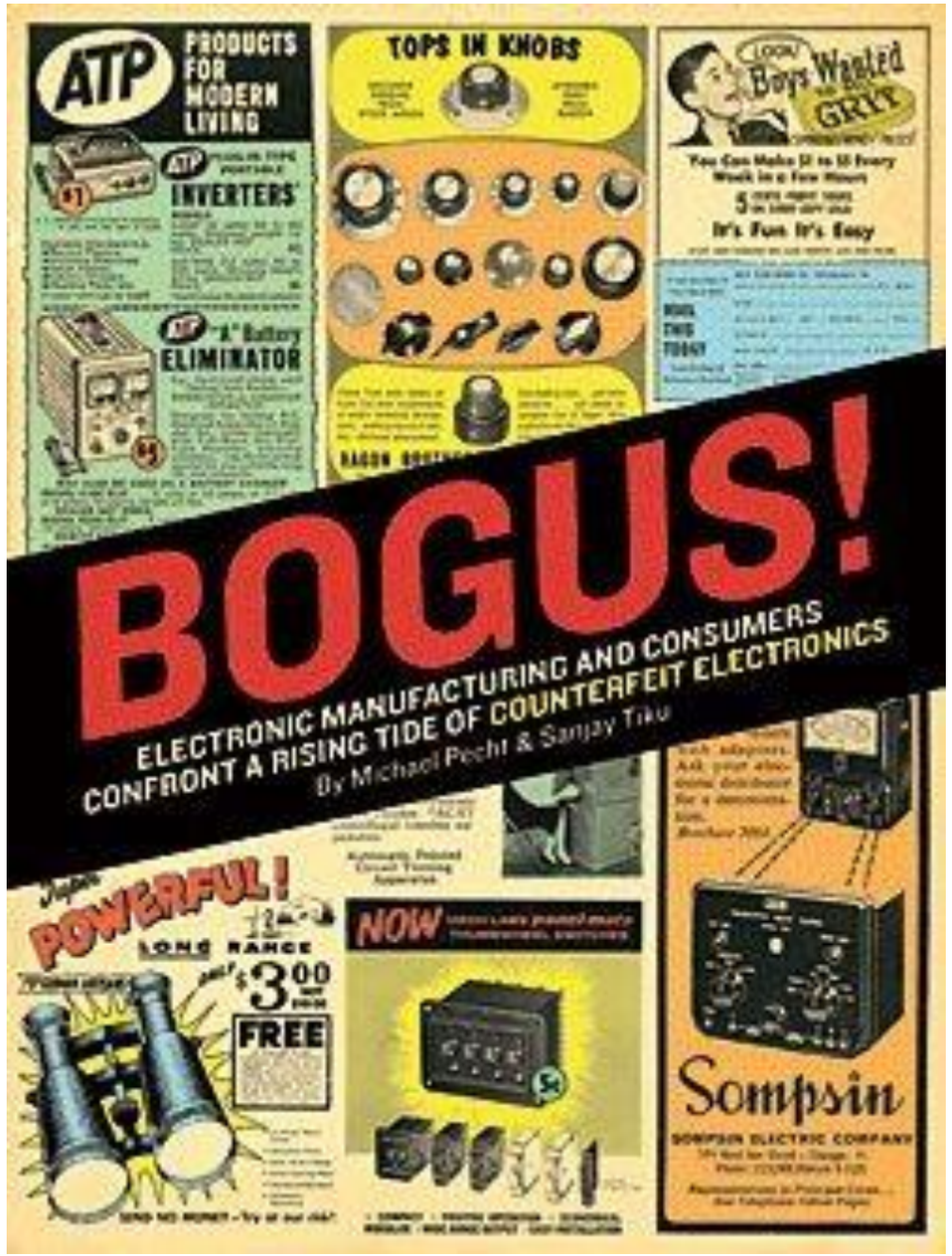
Electronic Counterfeiting

- Counterfeiting of electronics is a longstanding but evolving threat
- 2007 through April 2012: one counterfeit part reported every 15 second (source: Rory King, HIS, 2011)
- $169B estimated risk per year for global supply chain (source: IHS, 2011)
- Expensive and time-consuming to detect and replace (rule of ten)

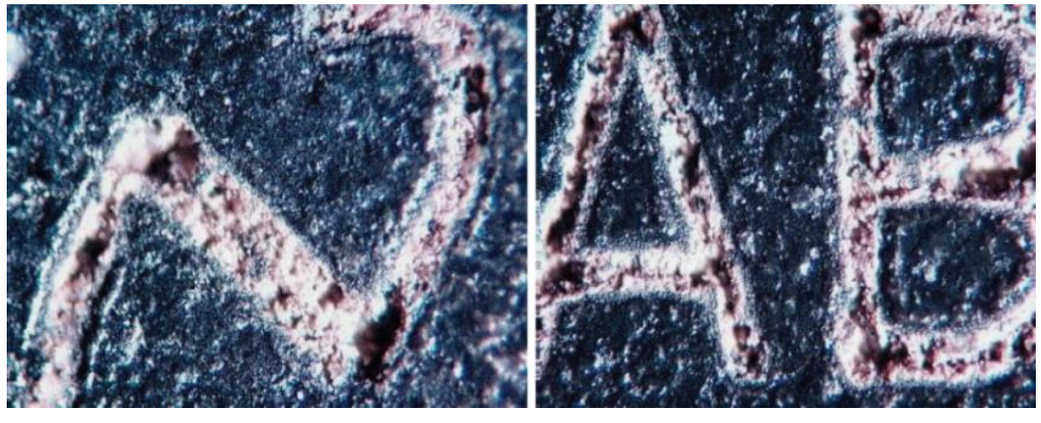
Top Part Type Reported in Counterfeit Incidents	Where Used → Industrial Market	Automotive Market	Consumer Market	Wireless Market	Wired Market	Compute Market	Other
Analog IC	14%	17%	21%	29%	6%	14%	0%
Microprocessor IC	4%	1%	4%	2%	3%	85%	0%
Memory IC	3%	2%	13%	26%	2%	53%	1%
Programmable Logic IC	30%	3%	14%	18%	25%	11%	0%
Transistor	22%	12%	25%	8%	10%	22%	0%

The top five represent $169 billion of semiconductor revenue in 2011, according to IHS iSuppli Application Market Forecast Tool (AMFT)

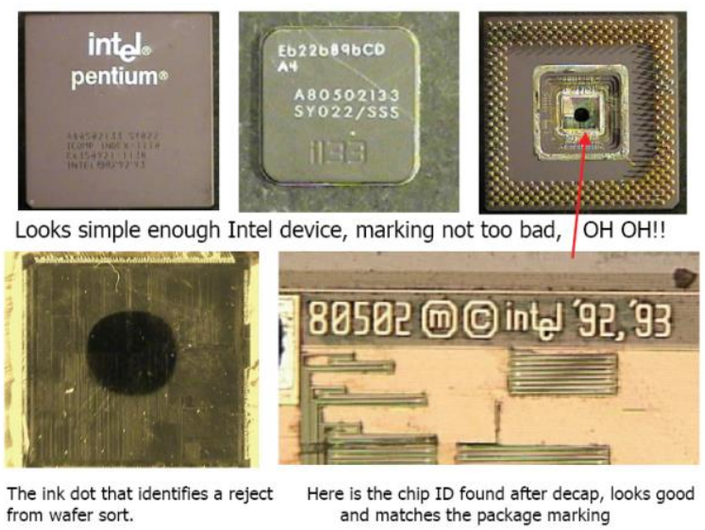
Source: IEEE Spectrum



What is a Counterfeit?



1) An unauthorized copy;
2) Does not conform to original chip manufacturer (OCM) design, model, and/or performance standards;
3) Not produced by the OCM or is produced by unauthorized contractors;
4) An off-specification, defective, or used OCM product sold as "new" or working; or
5) Possesses incorrect or false markings and/or documentation



Looks simple enough Intel device, marking not too bad, OH OH!!

The ink dot that identifies a reject from wafer sort.

Here is the chip ID found after decap, looks good and matches the package marking

Backside, look at the black shiny paint like substance in the lower right side, the mold pin cavity is almost gone, look at the bent leads, looks like it may have been painted over to hide sanding marks and then fraudulently remarked

U.S. Department Of Commerce, 2010

Impacts of Electronic Counterfeiting

1) **Public Safety and National Security:** Create risks for the critical systems and infrastructures that incorporate them



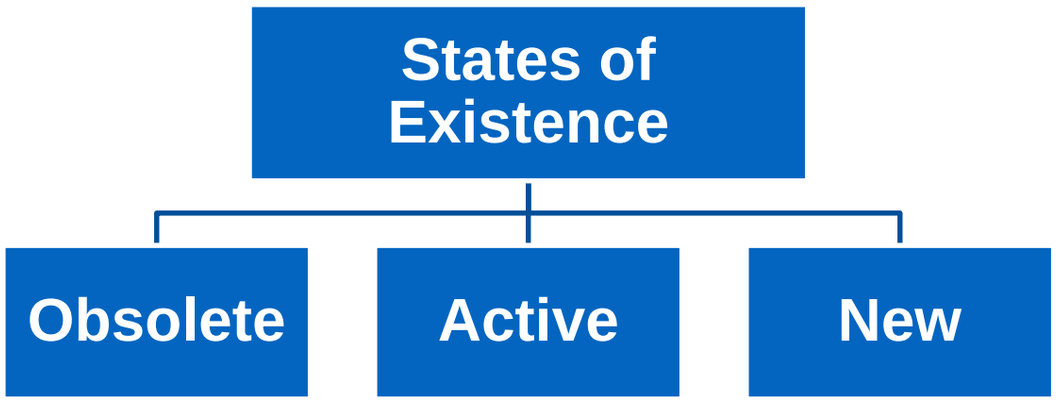
2) **Unfair Competition:** Irrecoverable economic losses for intellectual property (IP) holder – in sales, reputation, and replacement costs

3) **Criminal Financing:** Source of revenue for various groups, such as terrorist groups and organized crime


4) **Economy:** Enforcement costs, lost tax revenue, and reduced incentive to develop new products and ideas, thereby impacting job creation, employment, etc.

Source: Google Images

What Chips are Counterfeited?



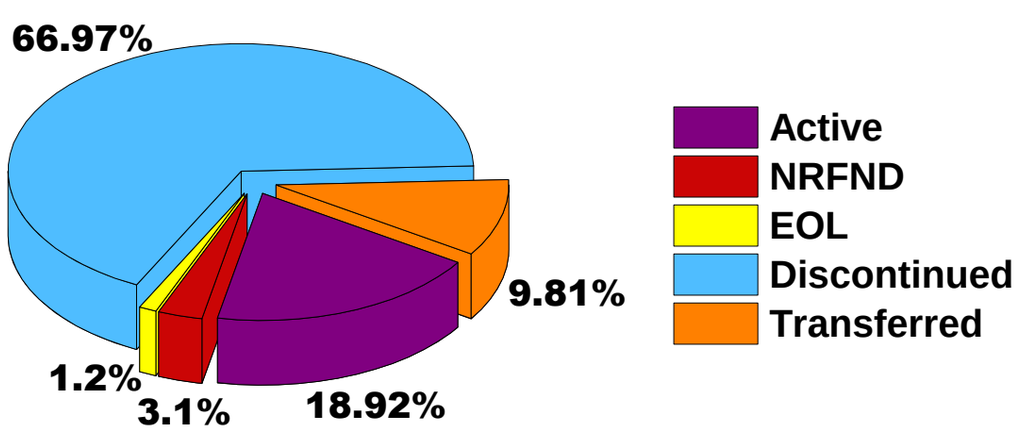
Analog and Mixed

- Transistors, diodes
- Amplifiers
- ADCs, DACs
- Mixers, etc.

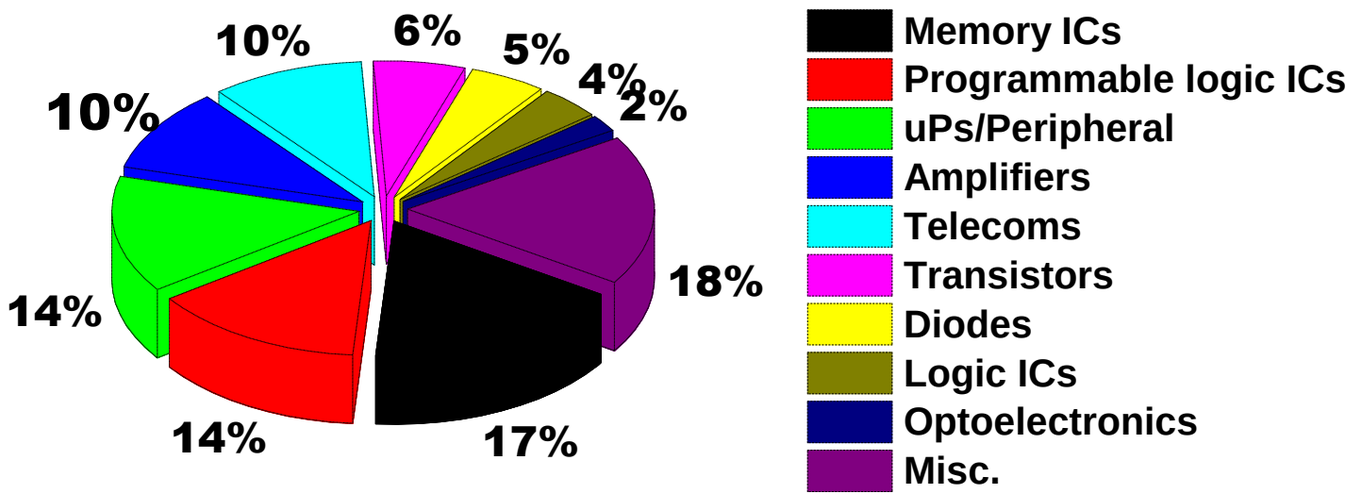
Digital

- µPs, µControllers
- DSPs
- FPGAs, CPLDs
- Memories

Source: IHS, 2016



Counterfeit by production status

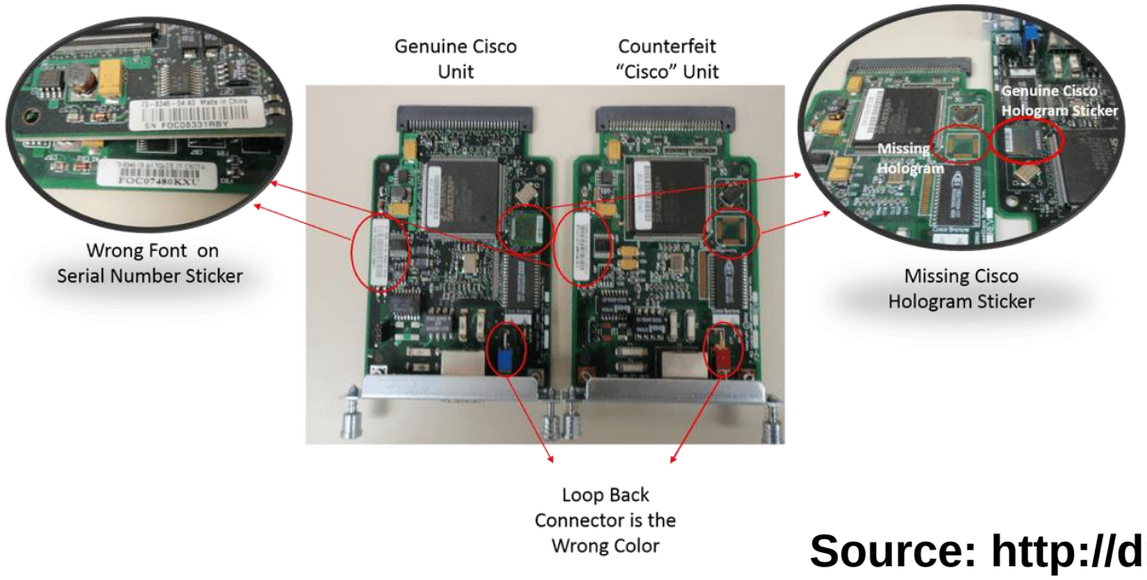


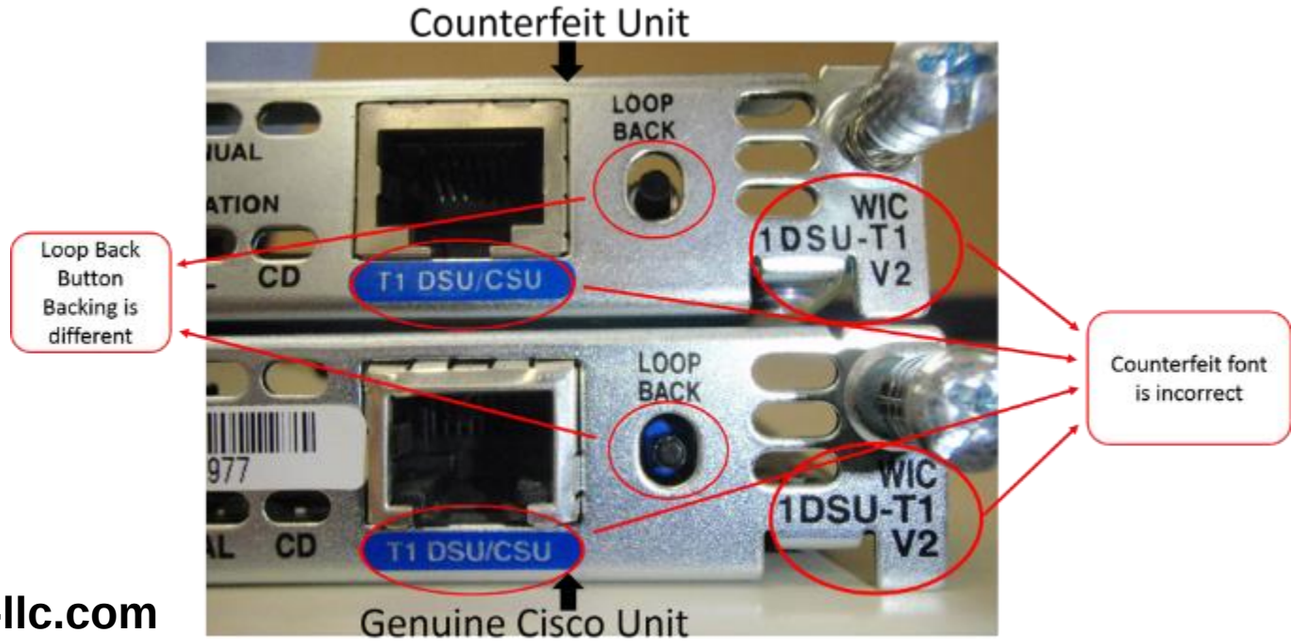
Counterfeit report by device type

Legacy systems are most heavily impacted - incentive

AMS most widely reported FPGAs and memories on the rise

Counterfeit Cisco Routers (2010)

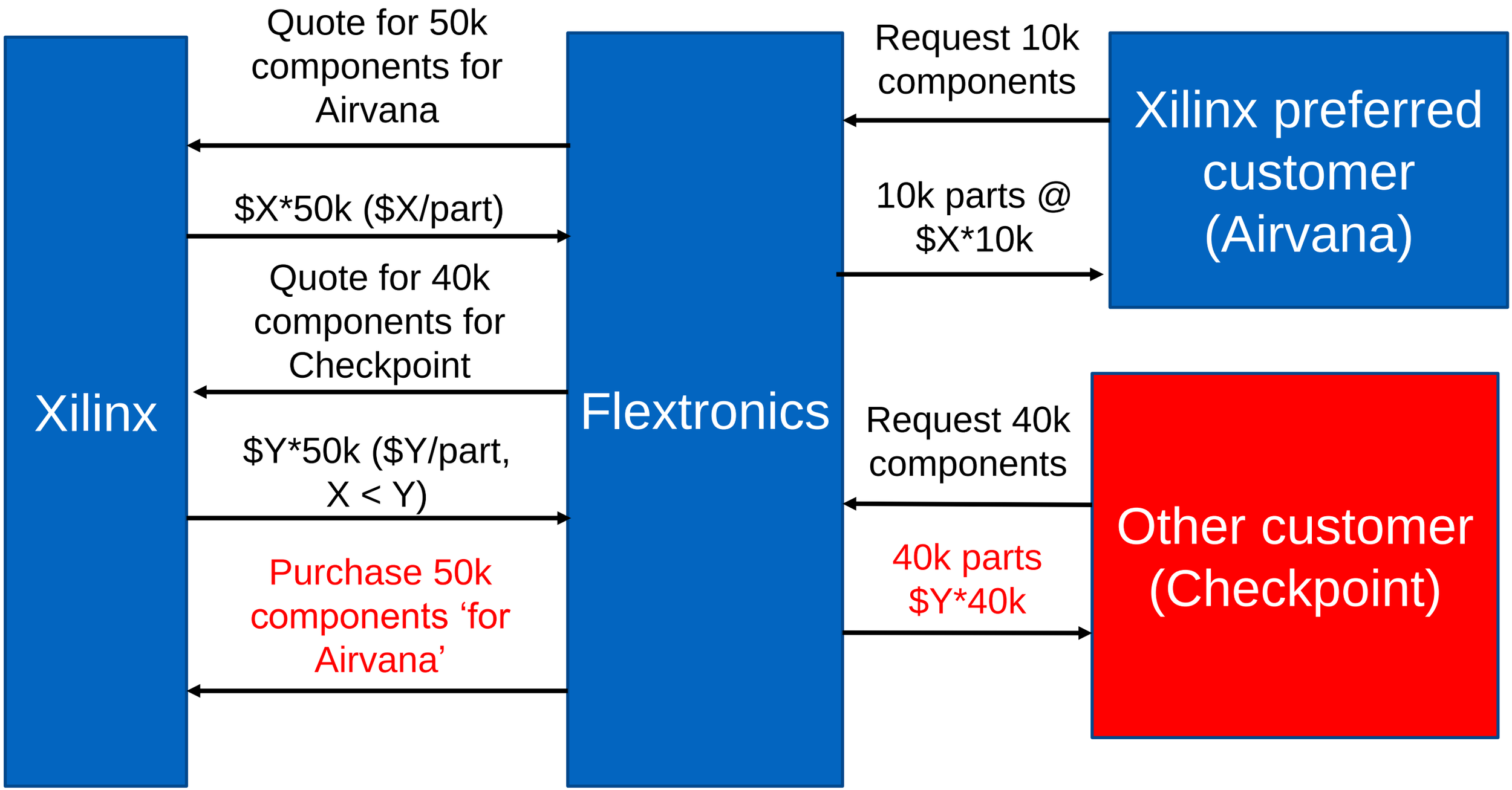




Source: http://dni-llc.com

- Thirty people were convicted of illegally distributing counterfeit Cisco equipment and intent to sell them to the U.S. Department of Defense
- The devices were to be installed in Iraq in Marine Corps networks used for security systems and for transmitting troop movements and relaying intelligence to command centers

Xilinx vs. Flextronics (2013)

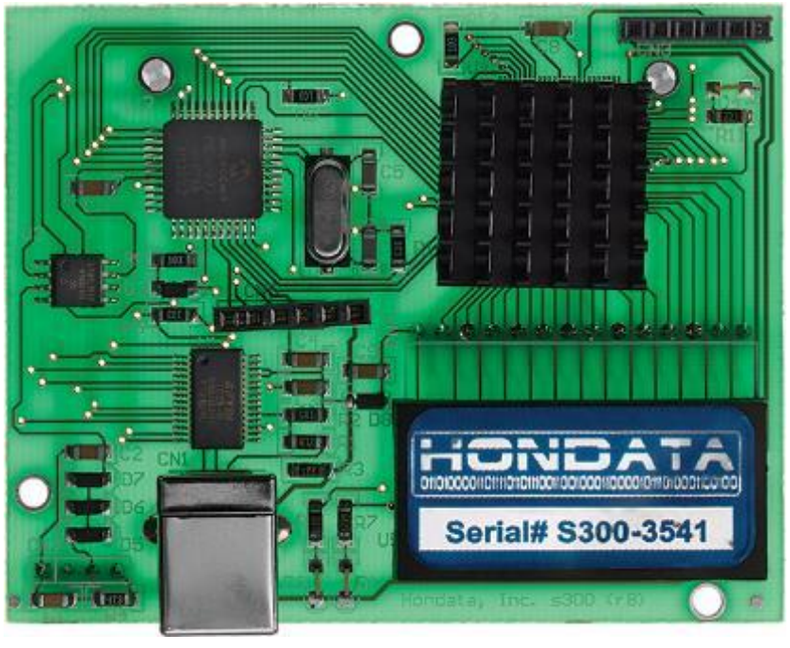


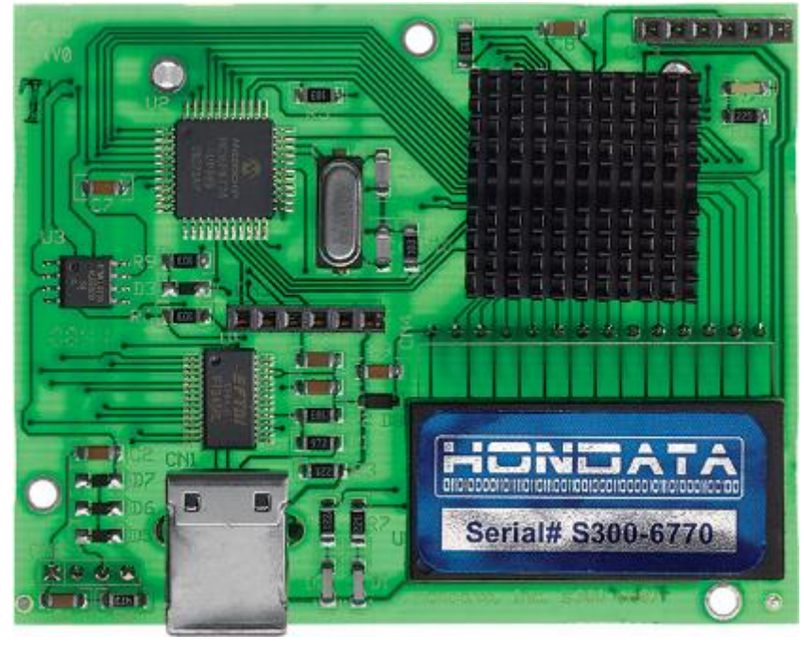
Flextronics Additional Profit / Xilinx Loss in Profit: $(Y-X)40k

https://epsnews.com

Counterfeit Hondata s300 (2014)

Can you spot the fake?





Photos: The Voorhes

- Hondata s300 reads data from sensors in Honda cars and automatically adjusts the air-fuel mixture, idle speed, and other factors
- PCBs were reverse engineered and built in China
- Counterfeit issues included random limits on engine rpm and, occasionally, failure to start
- Researchers have demonstrated that such devices (containing Bluetooth) connected to ECU could hijack a car's brakes and steering

And the Worst…

Parallel NEC Brand (2006)

Source: nytimes.com

- Counterfeiters set up 50 factories in China, Hong Kong, and Taiwan
- 50 products were copied in addition to developing their own

Fake Apple Store (2011)

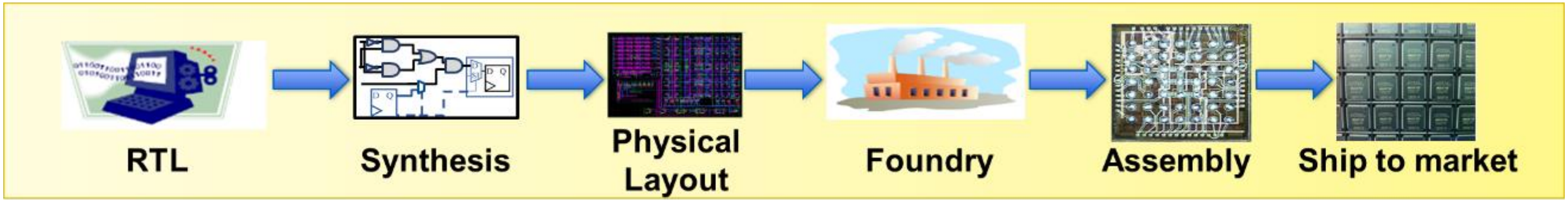
Source: businessinsider.com

- 30 fake Apple stores found in Shenzhen
- Even employees were fooled
- “Apple Store” written on signs

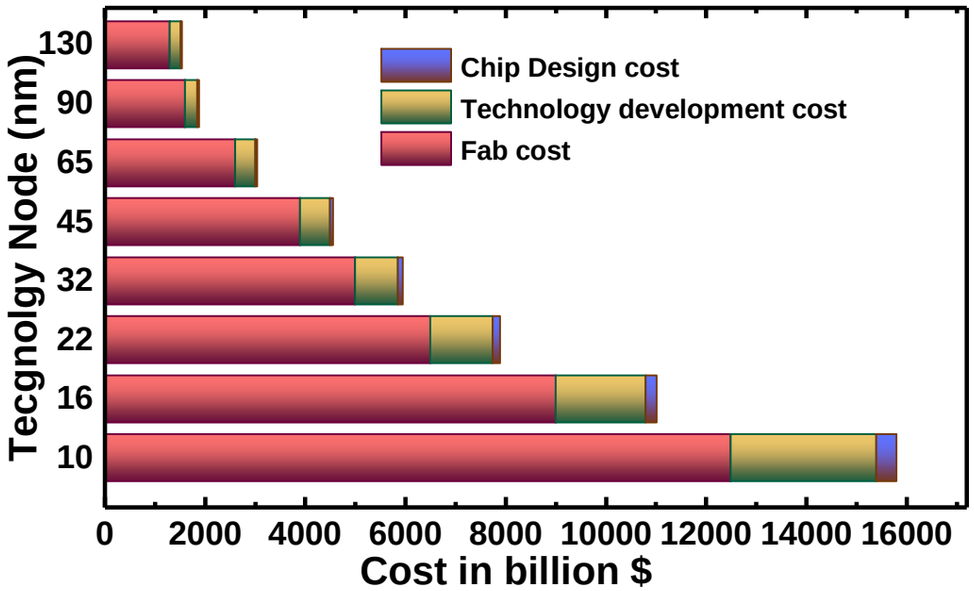
Section II: Adversarial Models and Counterfeit Taxonomies

Modern IC Supply Chain

Horizontal –Two or more companies involved



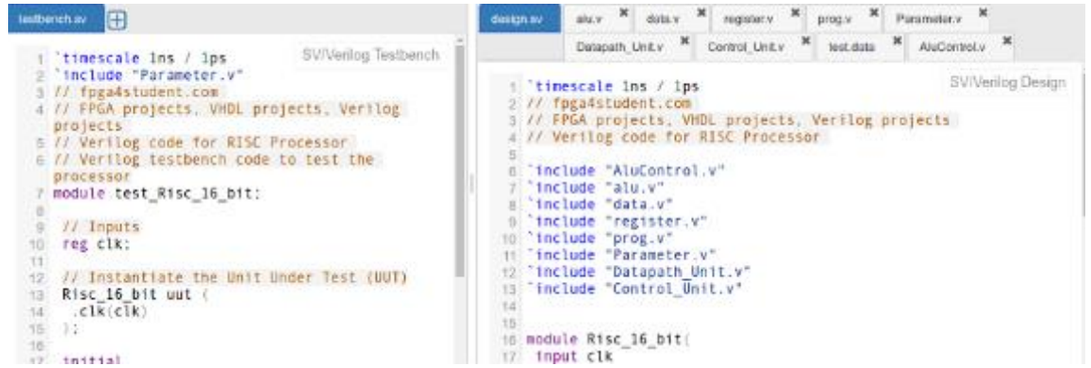
Source: semi.org



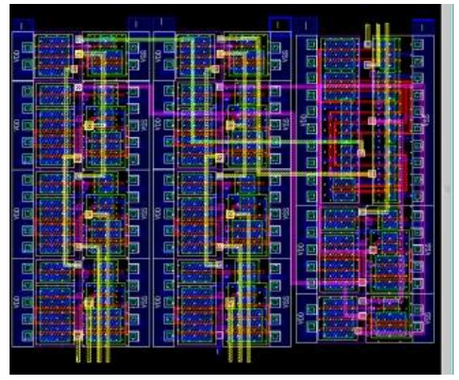
Globalization became essential to reducing design and fab costs

Semiconductor Intellectual Property (IP)

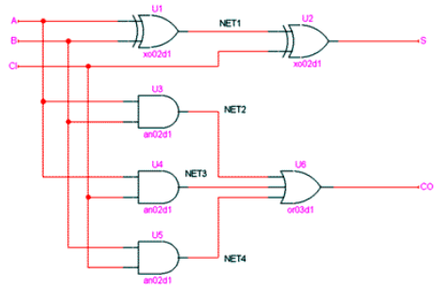
Semiconductor IP refers to a reusable unit of logic, cell, or chip layout design that is either licensed to another party or owned and used solely by a single party



1) **Soft IP** takes the form of an HDL/RTL; most flexible; can be easily ported



2) **Hard IP** are commonly in GDSII form and have predictable performance; more common in AMS applications



3) **Firm IP** come as fully placed netlists; compromise between soft and hard IP

Different methods for IP Theft

1) Complete reverse-engineering by deprocessing, which results in a full transistor netlist or even higher-level description **- *legal if for educational purposes***
2) Obtaining a copy of the final GDSII file sent to the foundry
3) Obtaining an illegal copy of the Verilog source code used to create the chip
4) Copying/using a piece of IP that is improperly licensed (e.g., overusing an IP, even if legally purchased)

*** Any of these could include making superficial changes to the IP/IC design before reselling/reusing it**

IC Reverse Engineering

Conventional Frontside

De-package IC

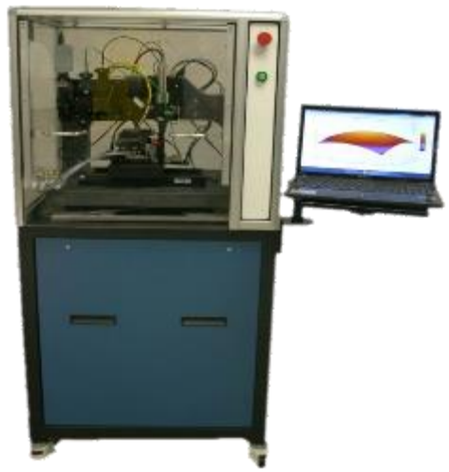
Clean & Prep (planarize)

Image Layer with SEM

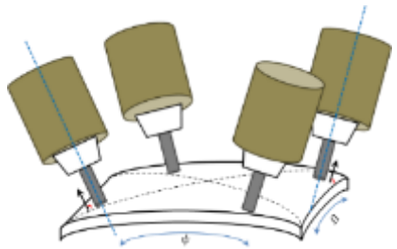
Remove Next Layer

Automated Plasma FIB Backside

(Principe et al., ISTFA 2017)



varioMill

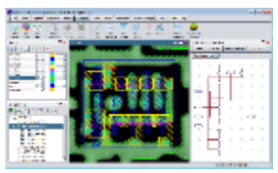


Backside 5 Axis Milling

Image Layer with SEM

Remove Next Layer

TESCAN FERA FIB-SEM



Extract IC Netlist

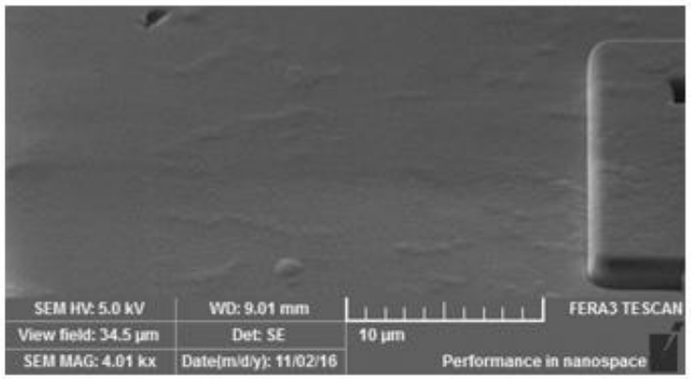
Texplained
HARDWARE SECURITY INSIGHT

Chipjuice

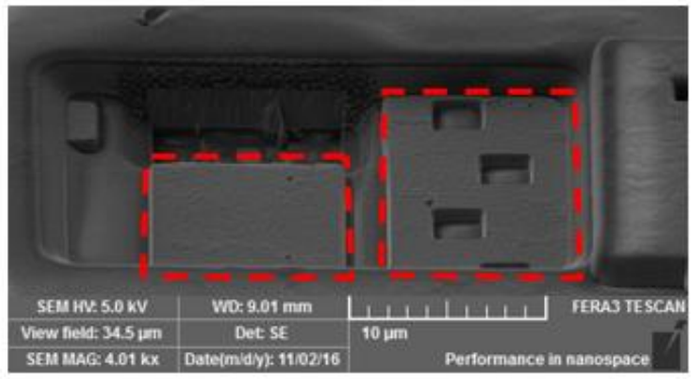
Pix2Net

MicroNet Solutions Inc.

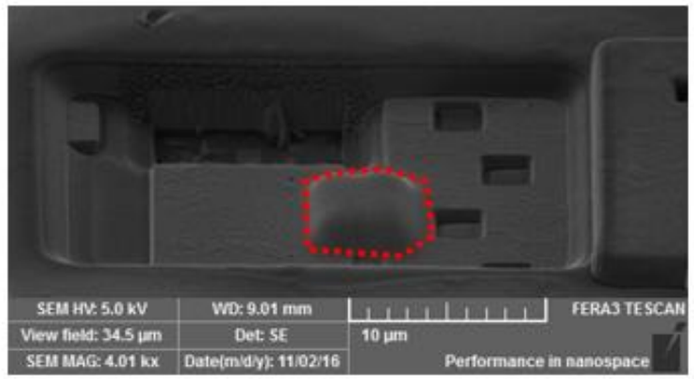
Focused Ion Beam (FIB)



Pre-FIB surface



FIB milling to expose adjacent interconnects



FIB deposition to short adjacent interconnects

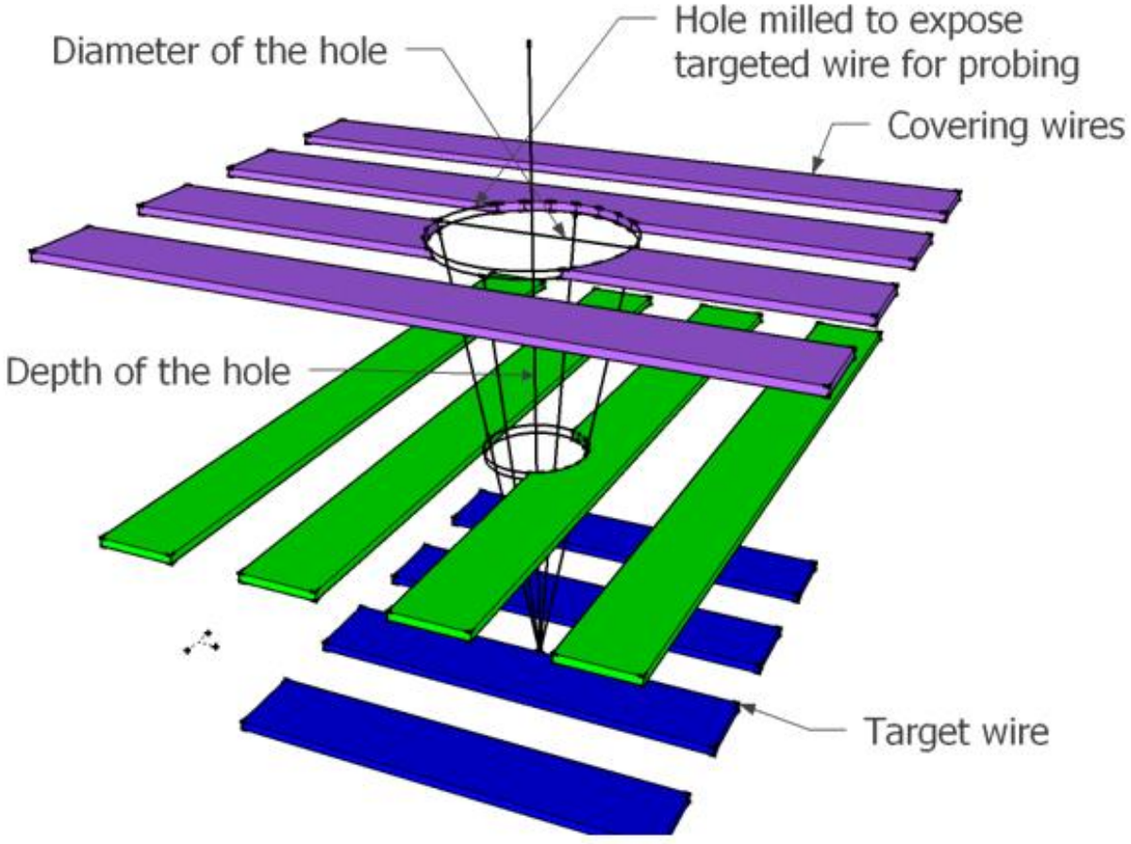
Source: FICS Research

Focused Ion Beam (FIB)

- A powerful tool commonly used in the development, manufacturing, and editing of ICs

Microprobing / editing Attack

- Probing at signal wires to extract security sensitive information
- Front-side attack and back-side attack



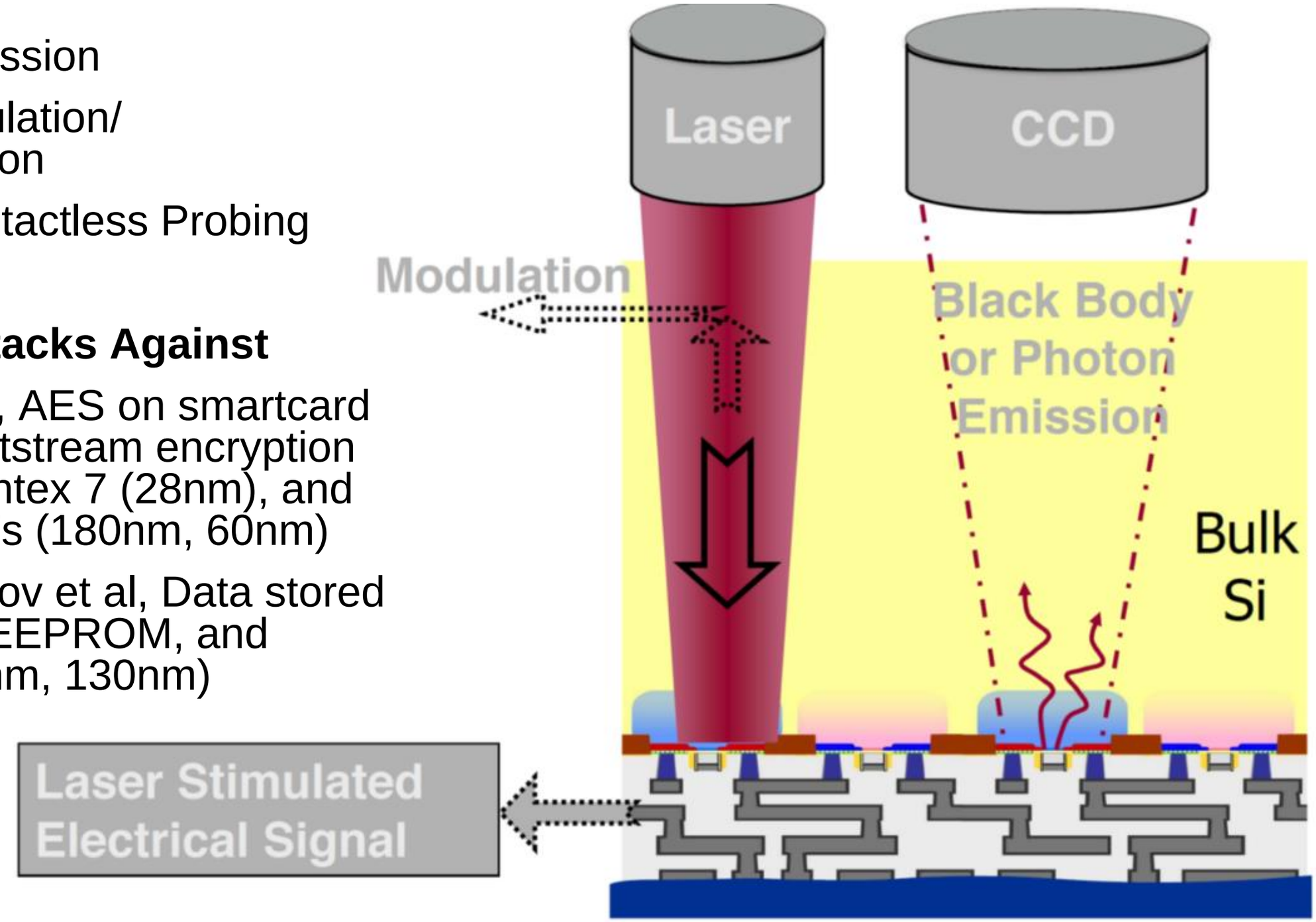
Optical Backside Attacks/Analysis

Methods

1) Photon Emission
2) Laser Stimulation/ Fault Injection
3) Optical Contactless Probing

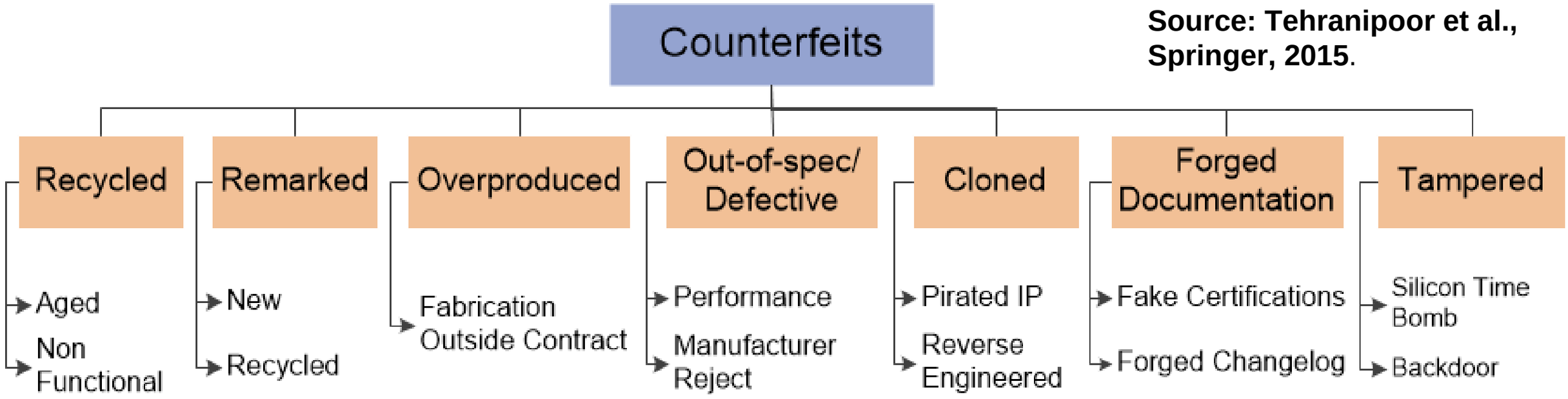
Successful Attacks Against

- Seifert et al, AES on smartcard (250nm), Bitstream encryption on Xilinx Kintex 7 (28nm), and Arbiter PUFs (180nm, 60nm)
- Skorobogatov et al, Data stored on SRAM, EEPROM, and Flash (900nm, 130nm)



Source: Tajik et al.

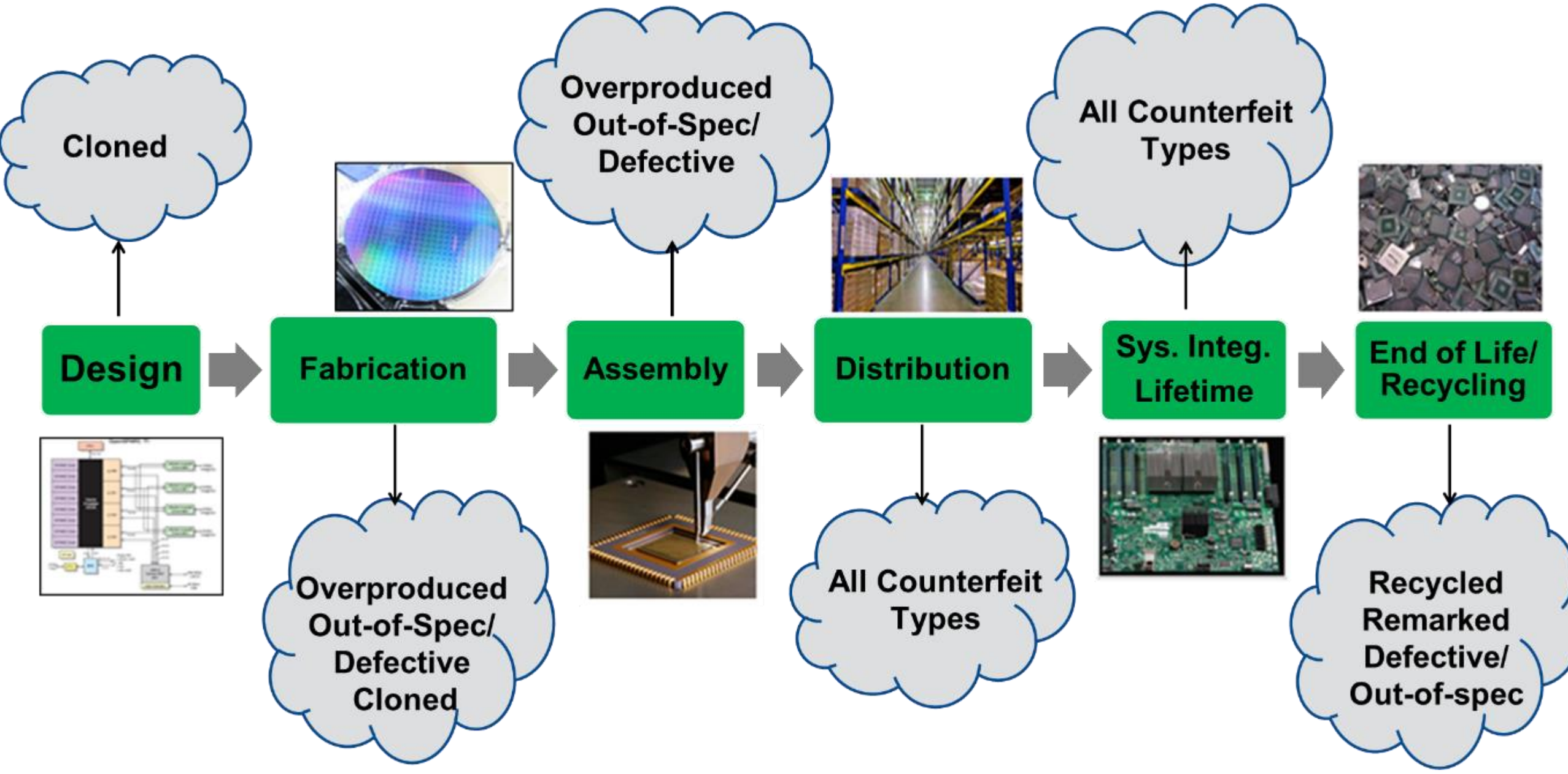
Counterfeit Chip Types



Source: Tehranipoor et al., Springer, 2015.

- **Recycled** and **remarked** types contribute to majority of counterfeit incidents
- Untrusted foundry/assembly can introduce **overproduced** and **out-of-spec/defective** parts
- **Cloning** can be done by a wide variety of adversaries (from small entities to large corporations)
- **Tampered** can include additional die and/or hardware Trojans within die

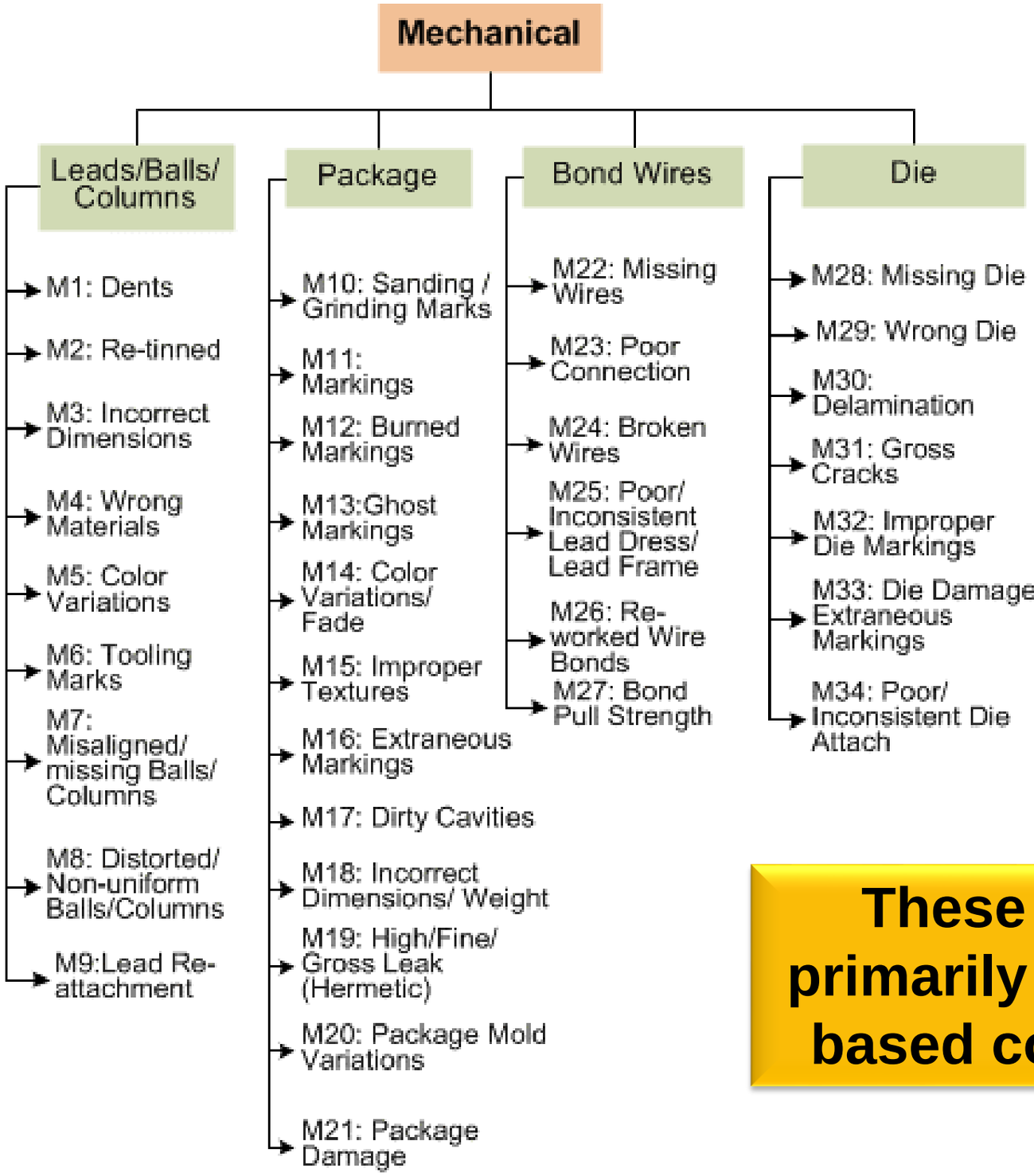
Electronic Component/System Vulnerabilities



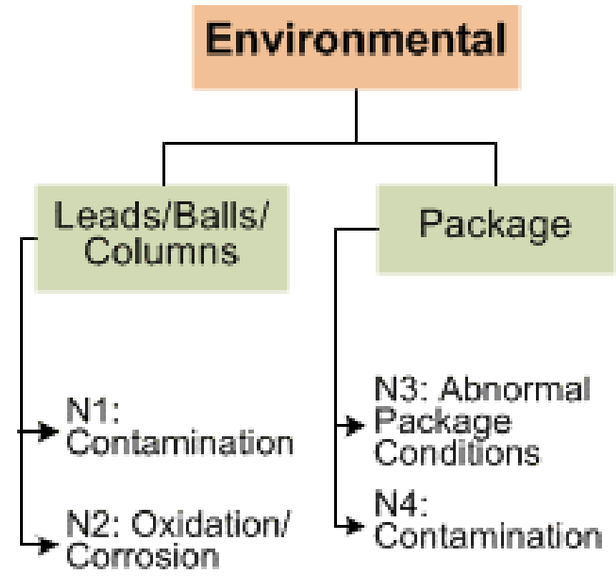
Kessler and Sharpe, 2010: Recycled type reportedly make up 80-90% of counterfeits

Source: Tehranipoor et al., Springer, 2015

Mech./Env. Defect Taxonomies

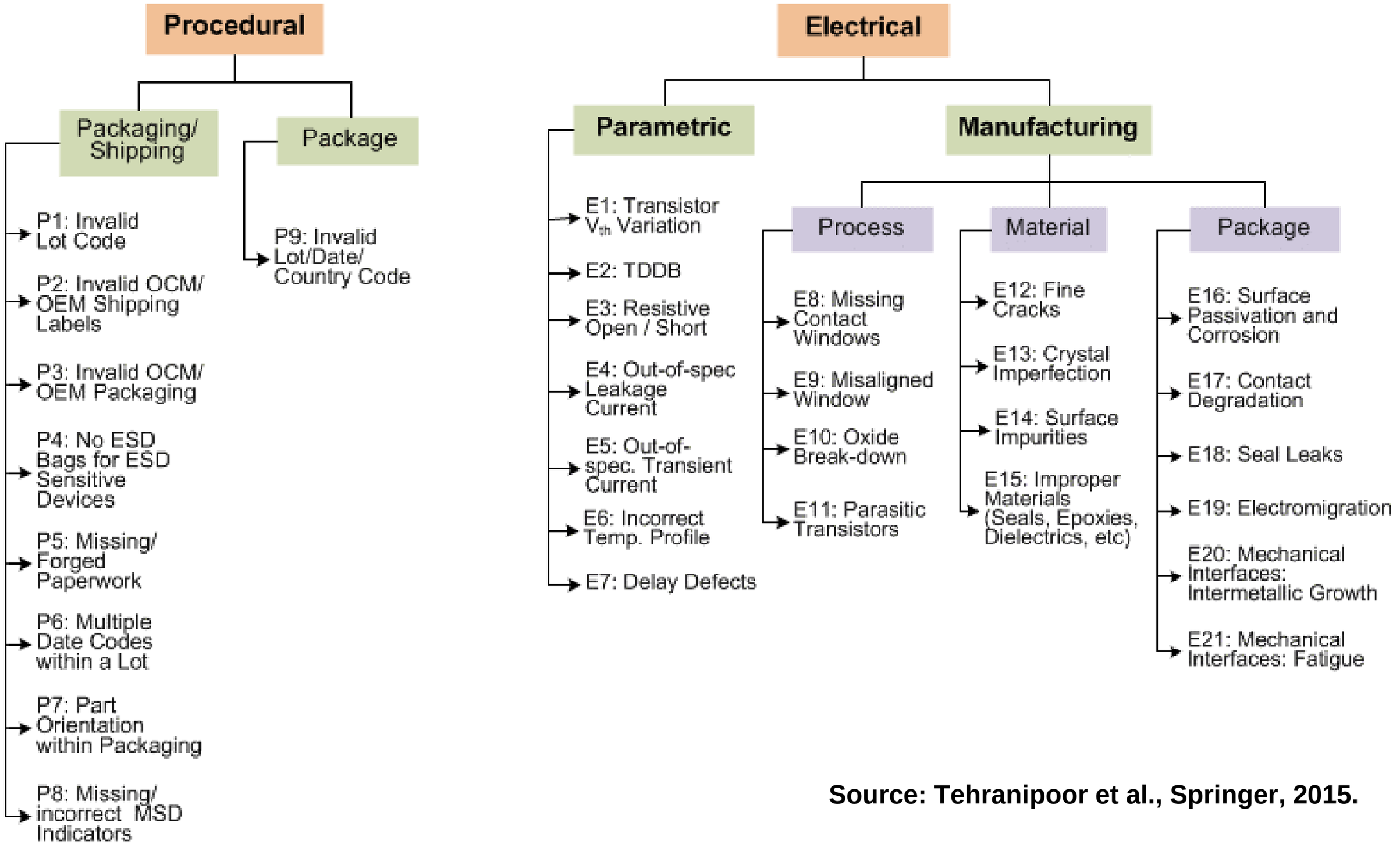


Source: Tehranipoor et al., Springer, 2015.



These two defect taxonomies are primarily used for physical inspection-based counterfeit detection methods

Proc./Elec. Defect Taxonomies



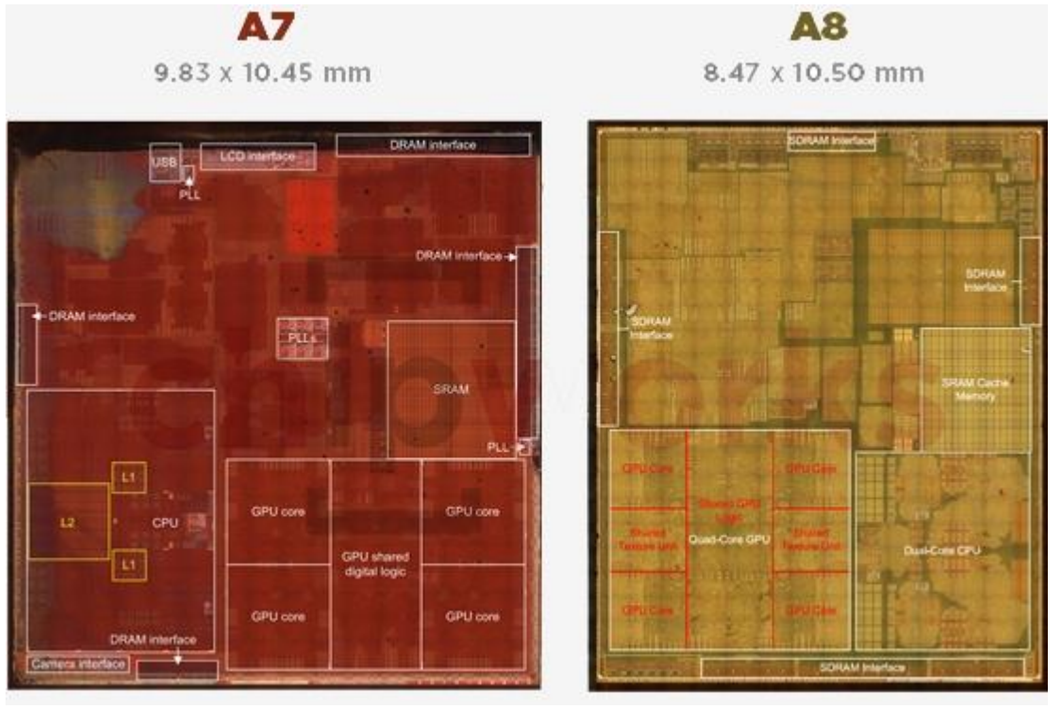
Source: Tehranipoor et al., Springer, 2015.

Section III: Counterfeit Detection Approaches

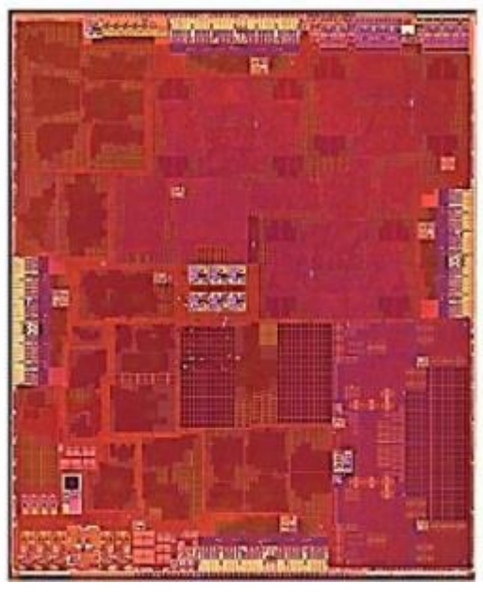
IP Services and Technology Analysis

- Reverse engineering for Tech Library to
  - Provide non-infringement evidence
  - Uncover patents to purchase
  - Find licensing opportunities
  - Build better patents
- Clients include 37 of the top 50 U.S. patent holders

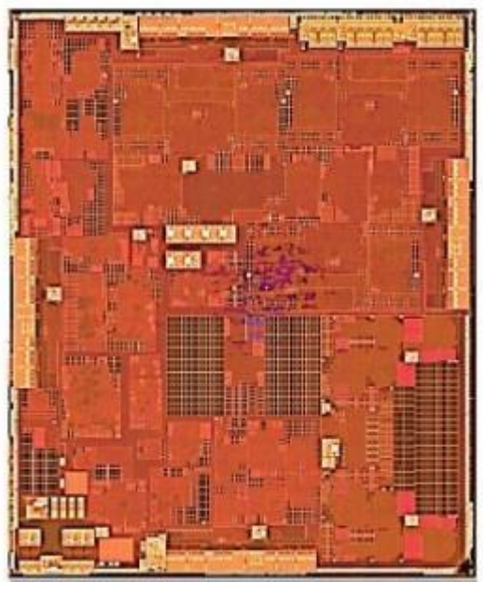
Apple iPhone Teardowns (Source: Chipworks)



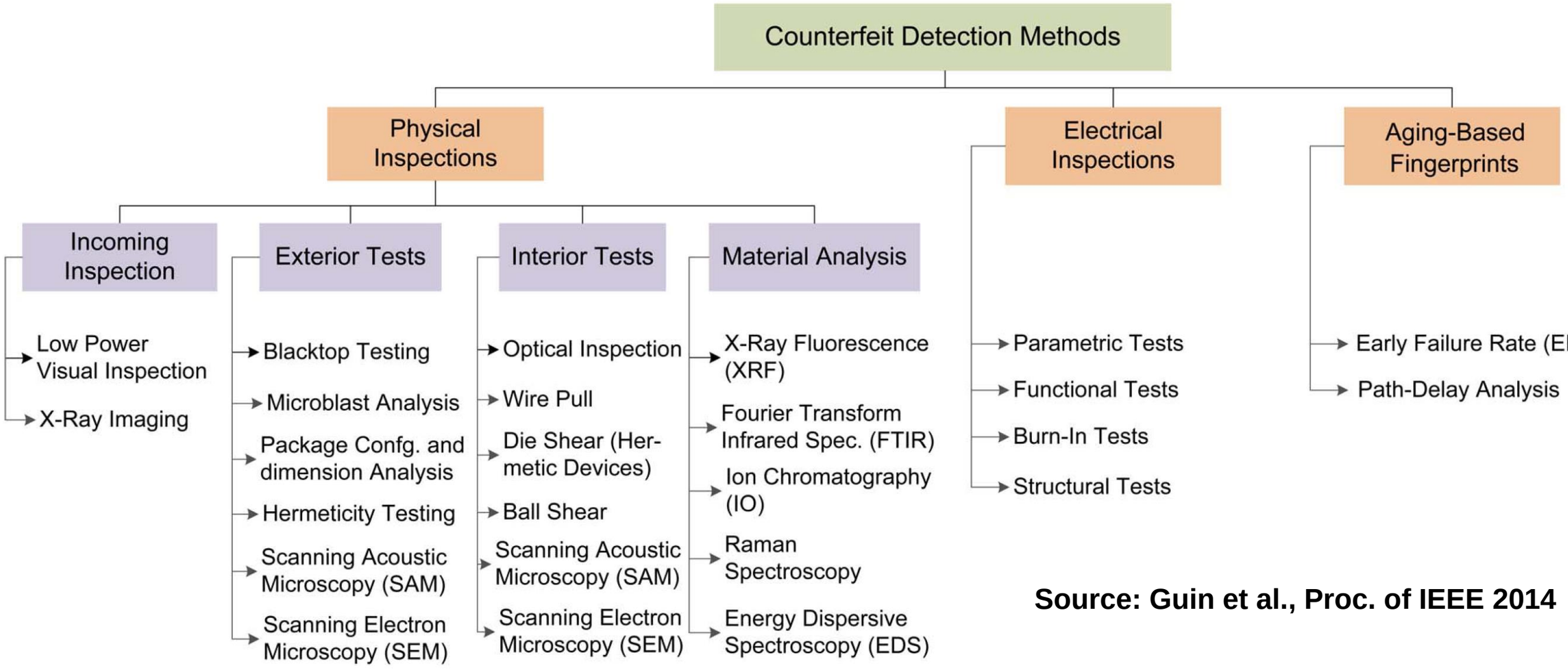
APL1022 – TSMC 16nm FinFET



APL0898– Samsung 16nm FinFET



Counterfeit Detection Taxonomy



Source: Guin et al., Proc. of IEEE 2014

Remarked and Recycled are well-covered by this taxonomy
Out-of-Spec/Defective, Cloned, and Tampered are partially covered

IC Recycling Process

A recycling center

PCBs taken off of electronic systems

ICs taken off of PCBs

Critical applications

Resold as new

Refined recycled ICs

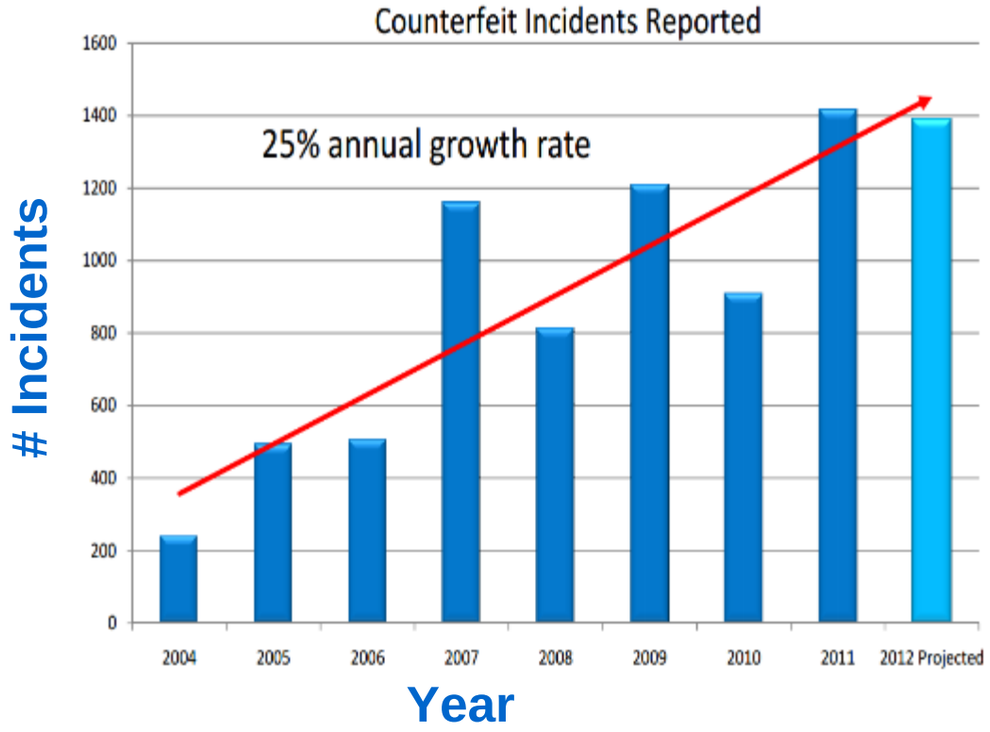
Source: Tehranipoor et al,, Springer, 2015

Consumer trends suggest that more gadgets are used in much shorter time – more e-waste

Recycled and Remarked ICs

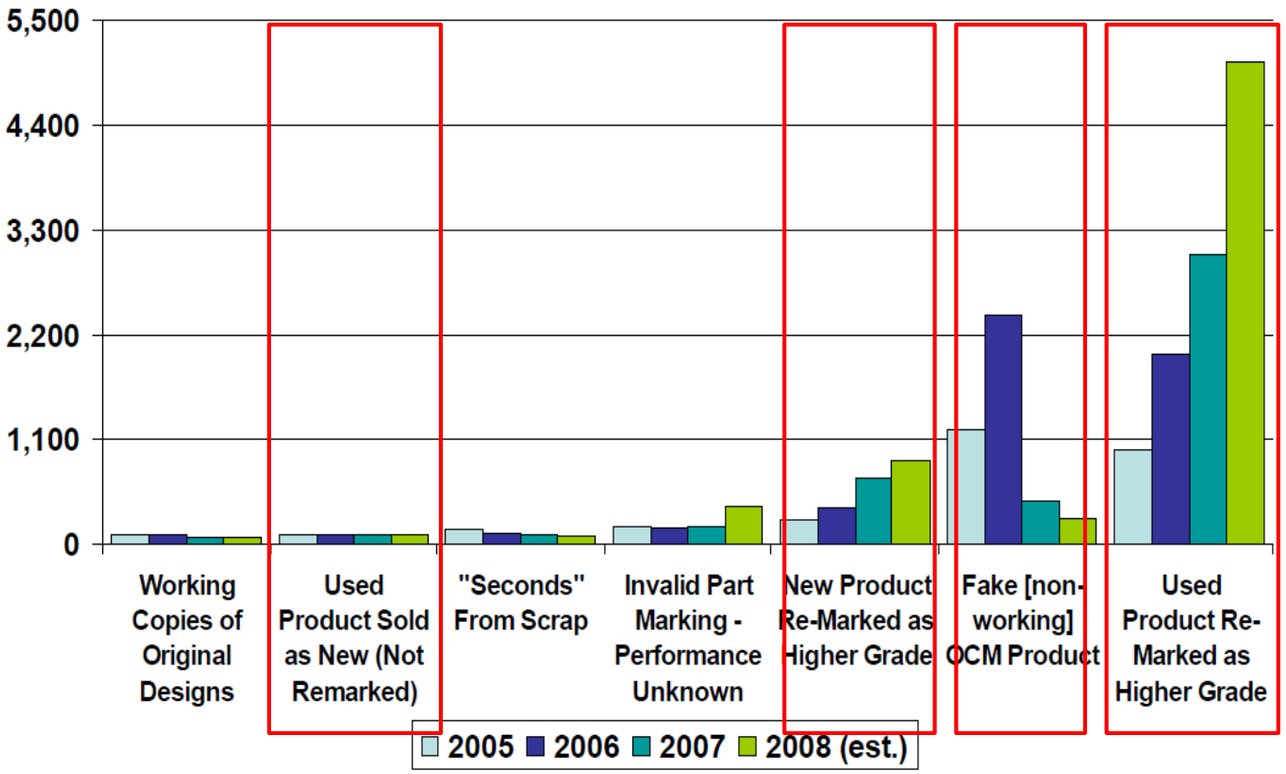
- Recycling and remarking of ICs have become major security and reliability problems
- IC Recycling: $15~$20 billion every year

IHS: All counterfeit incidents since 2004



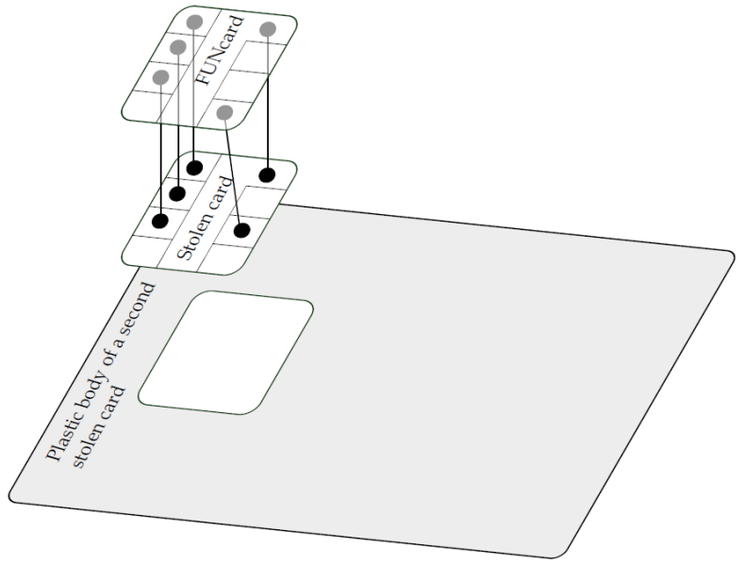
Source: IHS, 2011

Source: US Dept. of Commerce, 2009.



Counterfeit type incidents in 2005-2008 reported by US Dept of Commerce Bureau of Industry and Security Office

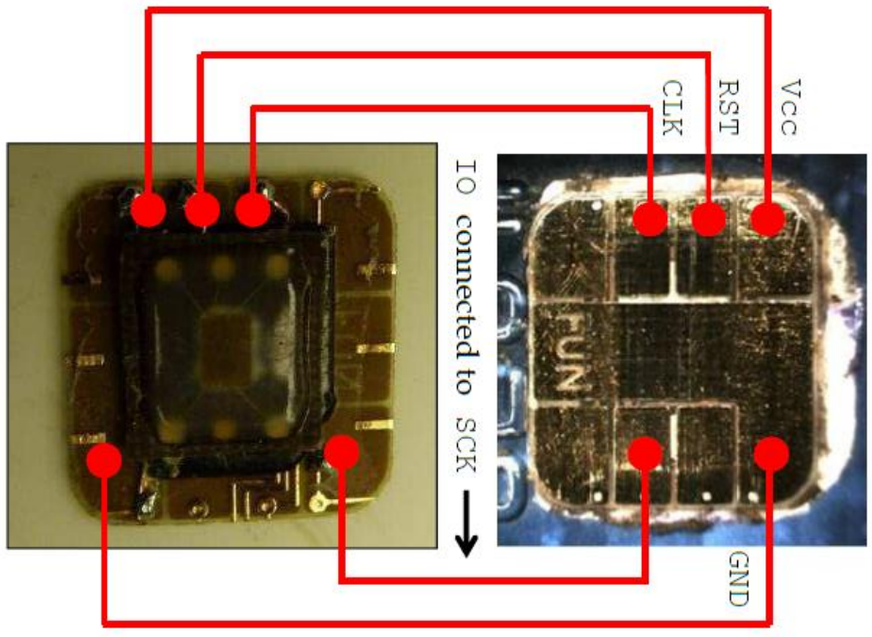
Tampered IC/EMV card Example

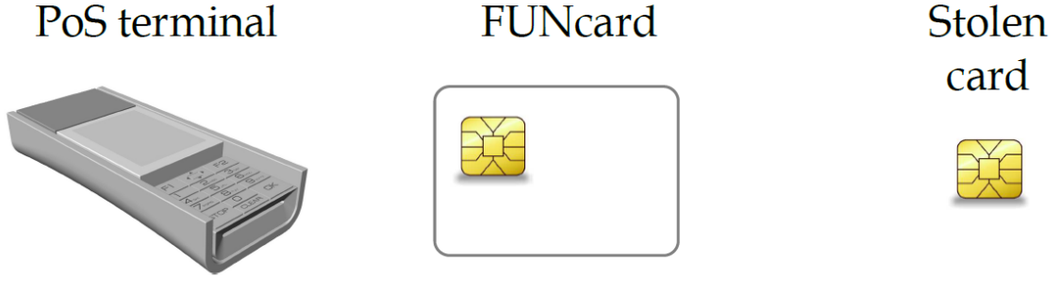


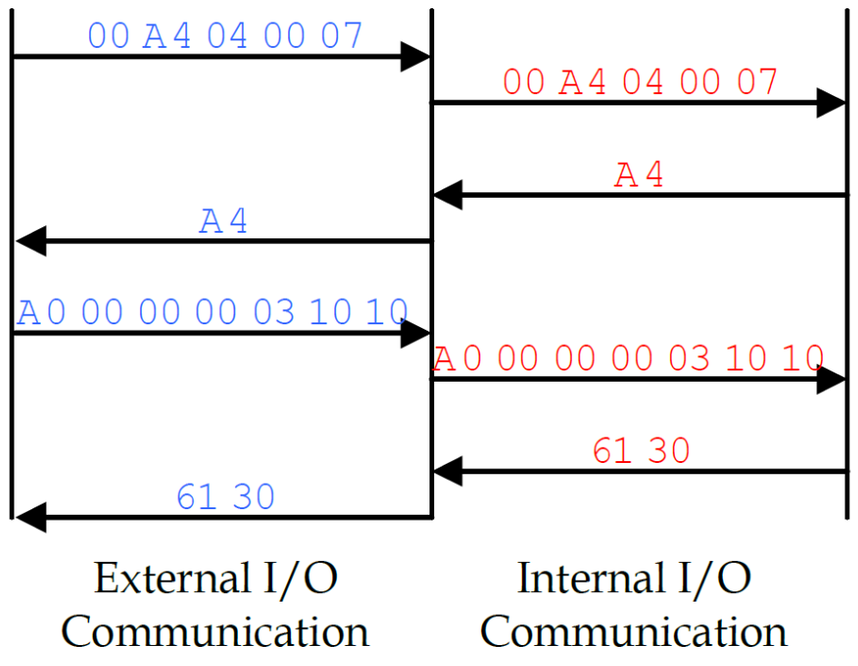
- **2010:** Murdoch et al. describe a man-in-the-middle attack against EMV cards
- **2011:** 40 sophisticated card forgeries resulting in ~ €600,000 net loss found

Forgeries embed two chips wired top-to-tail (stolen EMV and "FUN card)

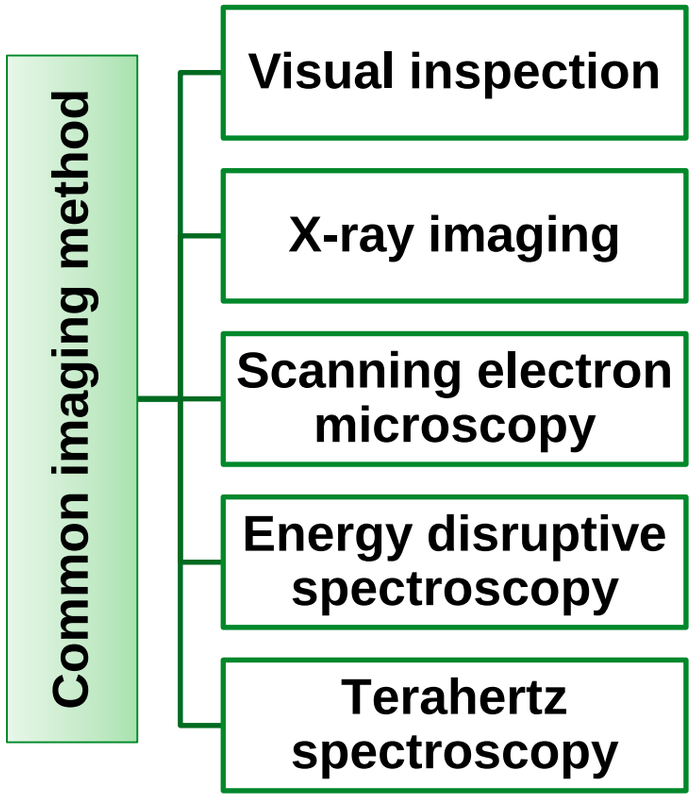
Source: Ferradi et al., Journal of Cryptographic Engineering, 2016





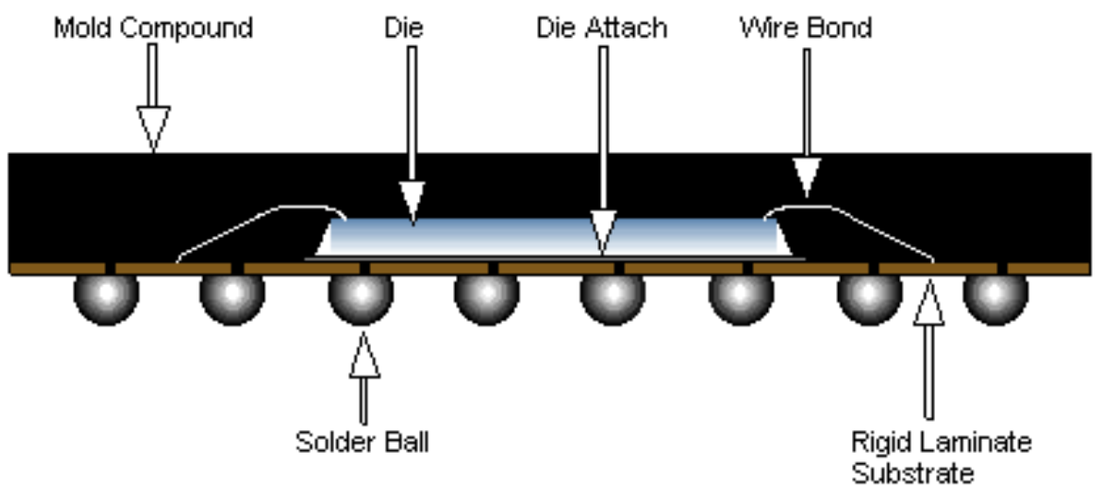


Physical Inspection

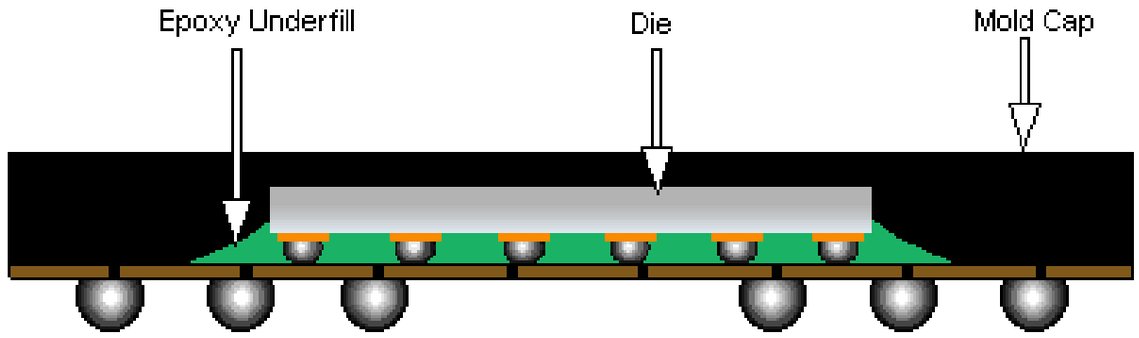


- Analyze the **physical properties** of a component
  - **Incoming inspection**: LPVI, X-ray imaging (XRM)
  - **Exterior/Interior tests**: X-ray CT, SAM, SEM, THz
  - **Material analysis**: XRF, FTIR

WIRE BOND

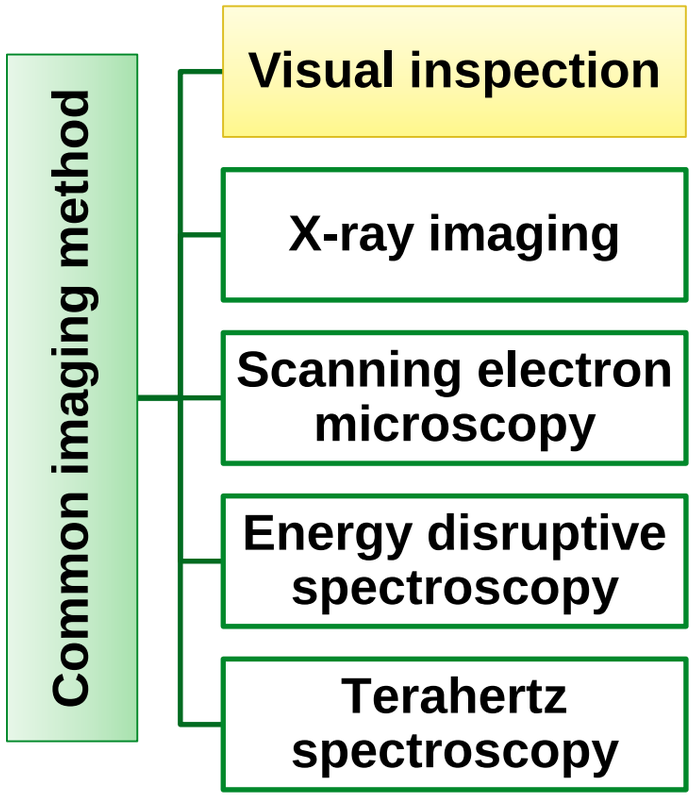


FLIP CHIP



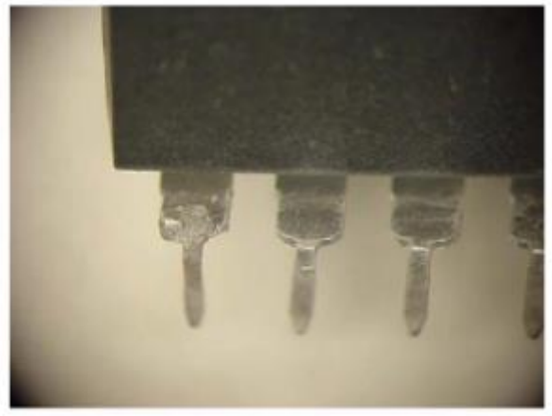
Source: pcmag.com

Low-Power Visual Inspection (LPVI)



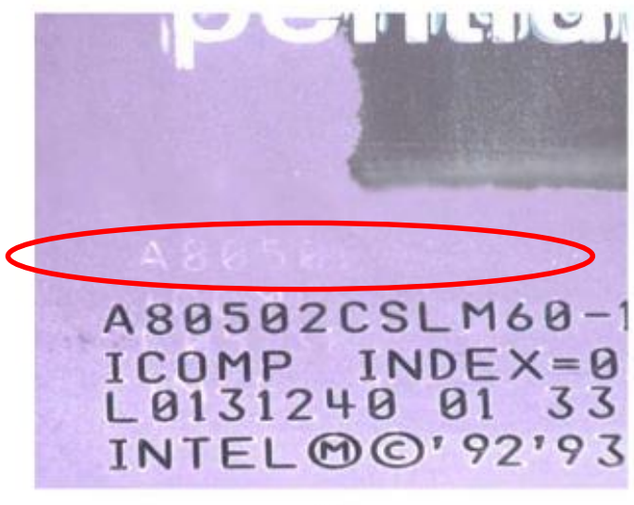
- First test usually performed on all the components
- Using a low-power microscope (less than 10X)

Peeled off lead plating



Residual material indicates reworking

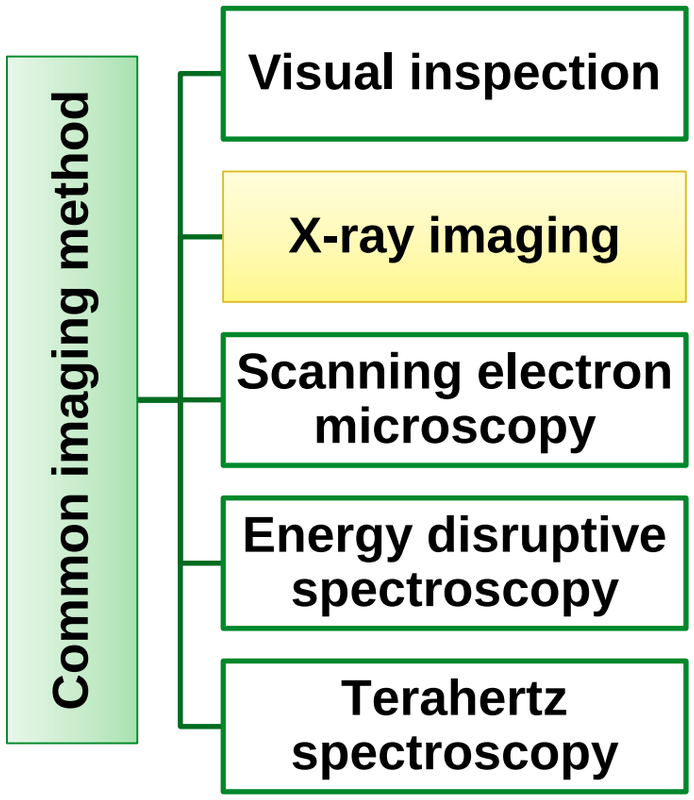
Source: Honeywell



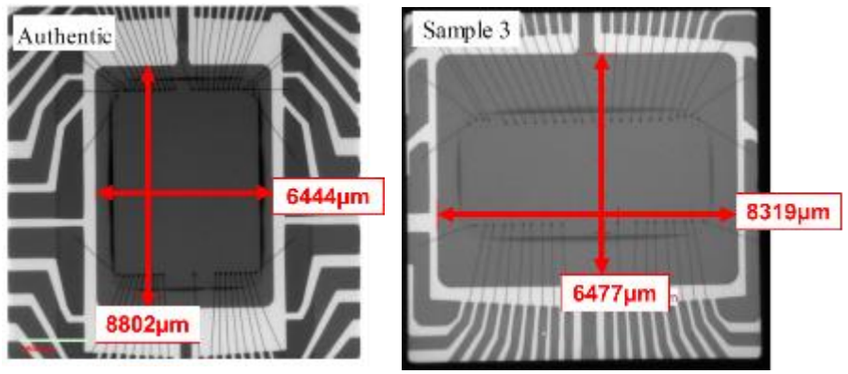
Ghost markings

Heat sink mark indicating prior usage

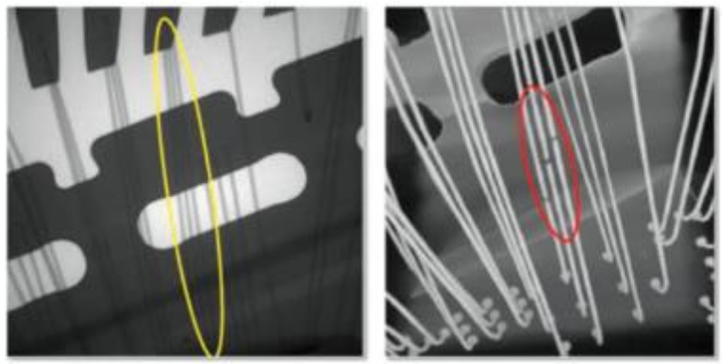
X-Ray ‘Nondestructive’ Imaging



- **Radiography** generates 2D image showing internal features of sample
- **Computational Tomography (CT)** generates a 3D representations from multiple 2D projections

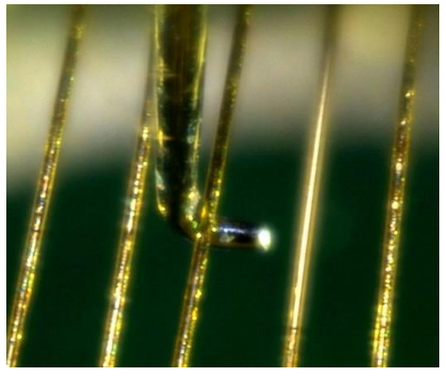


Different die (orientation, size) and lead frame (source: Shahbaz et al., ISTFA 2014)



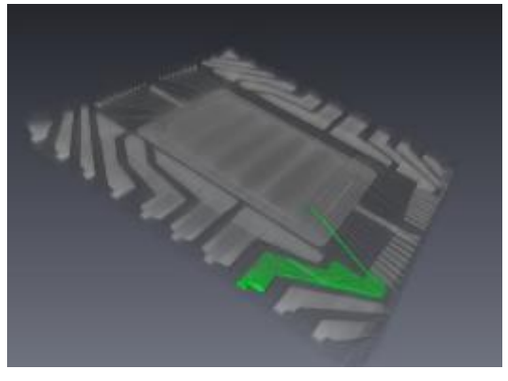
Broken bond wires only visible in 3D (right, source: Shahbaz et al., ISTFA 2014)

Traditional Bond Pull Test

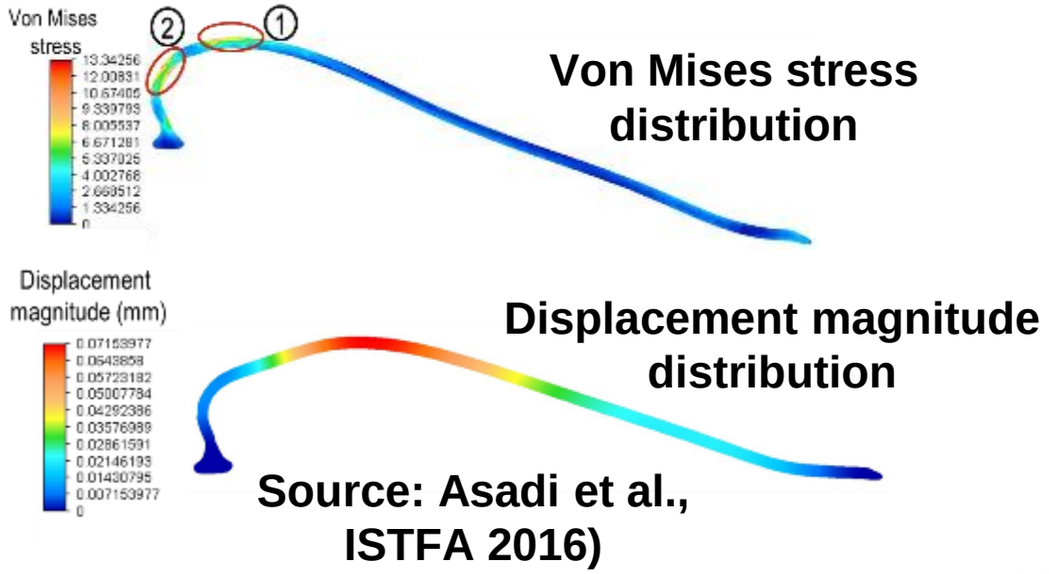


Source: xyztec.com

Virtual Bond Pull Test



FEM

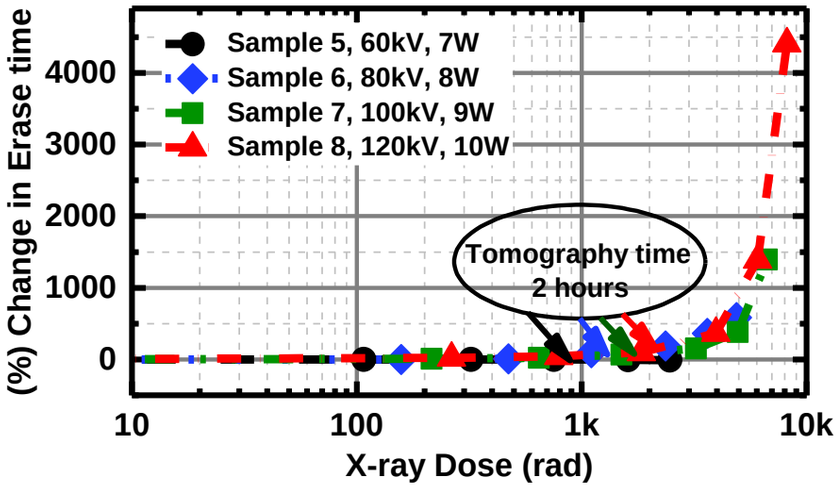


Von Mises stress distribution

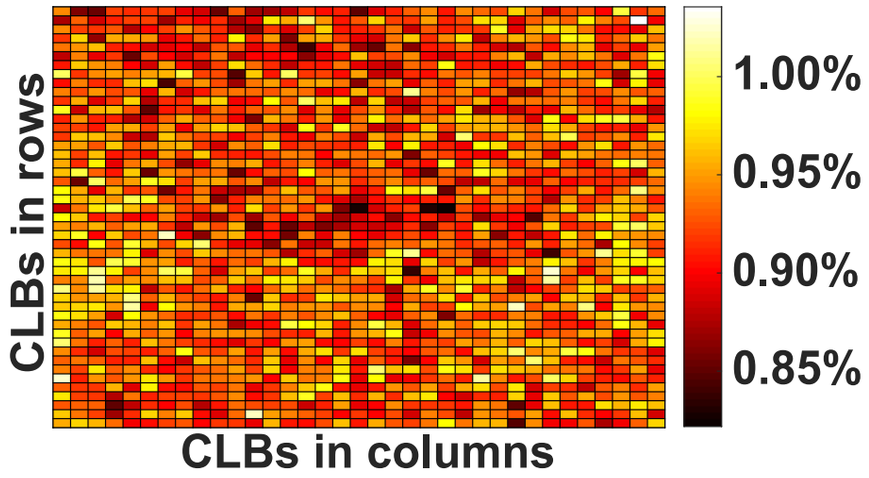
Displacement magnitude distribution

Source: Asadi et al., ISTFA 2016)

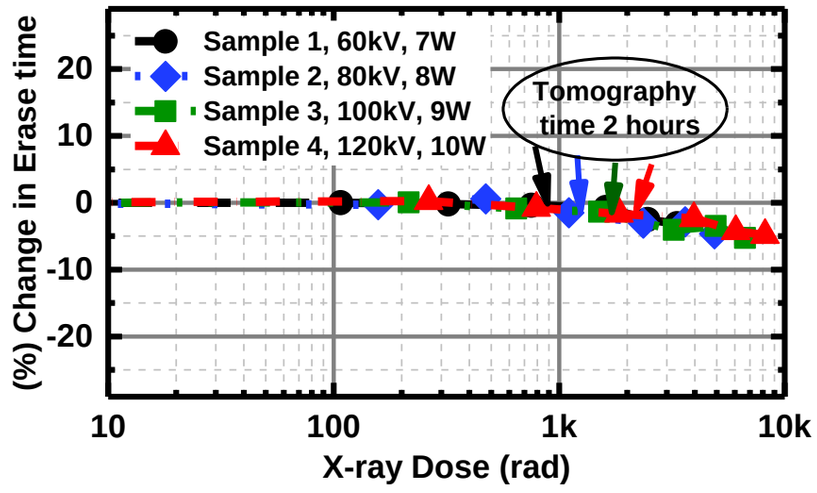
Impact of Radiation



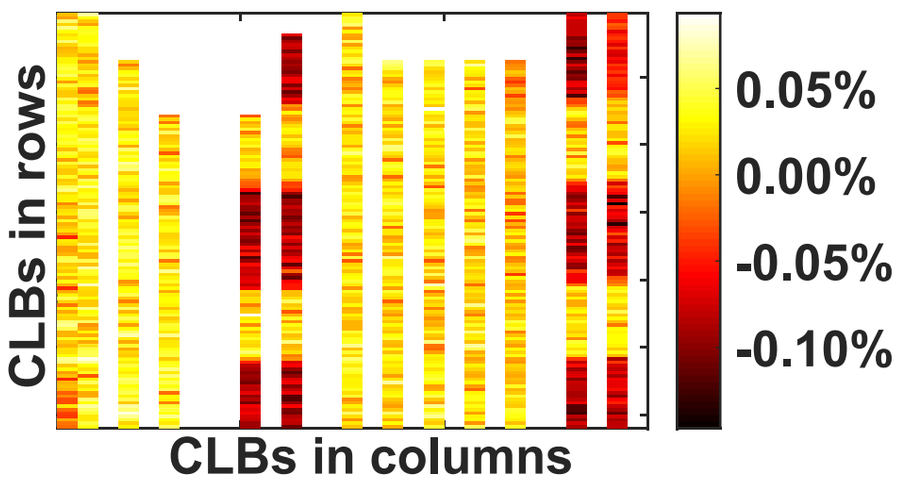
Change in erase time in Intel Flash (400nm)



Delay degradation in Spartan-3 at 10k dose



Change in erase time in Macron Flash (150nm)



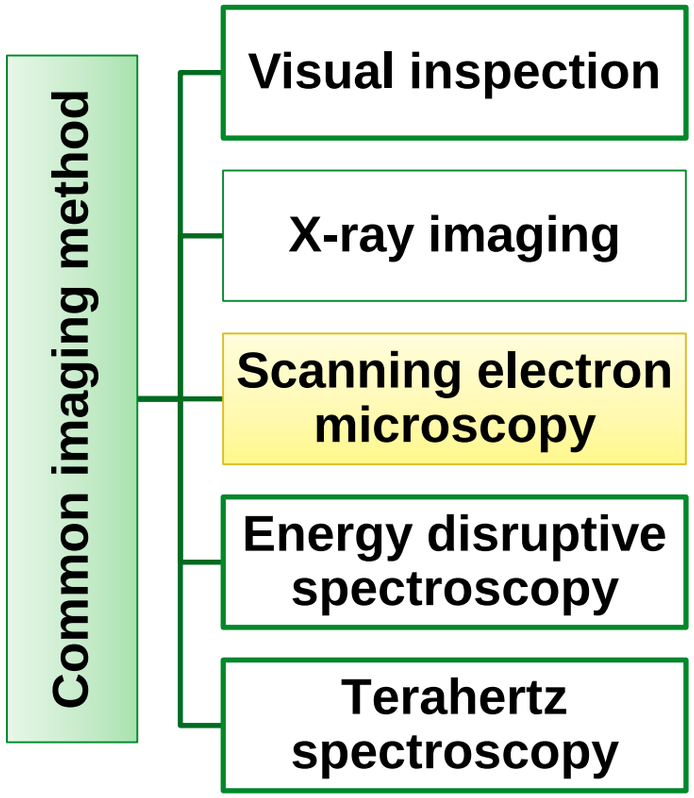
Delay degradation in Spartan-6 at 10k dose

Significant degradation observed in Flash manufactured in older technology nodes

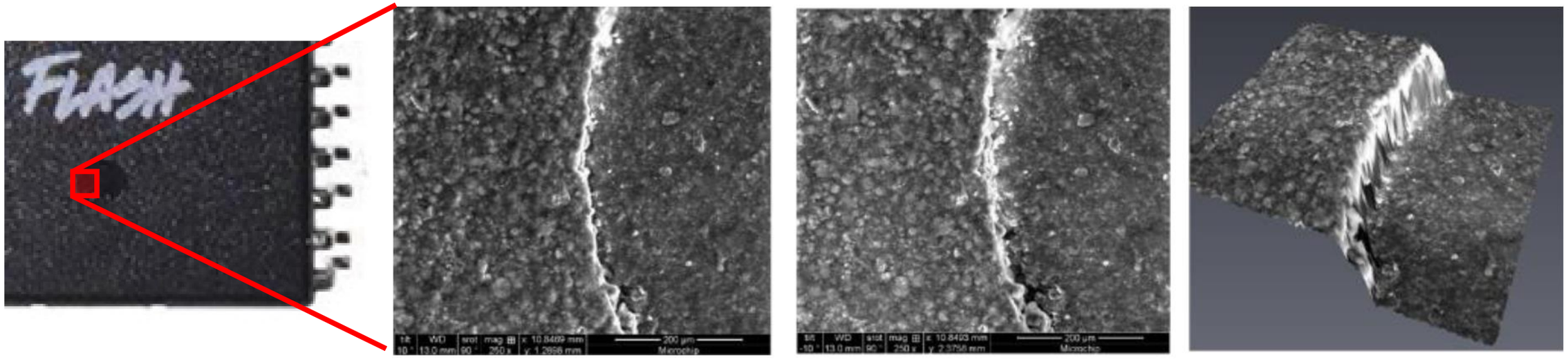
Frequency of FPGAs (90nm and 45nm) exhibits negligible change

Source: Alam et al., TDMR 2017

Scanning Electron Microscopy (SEM)

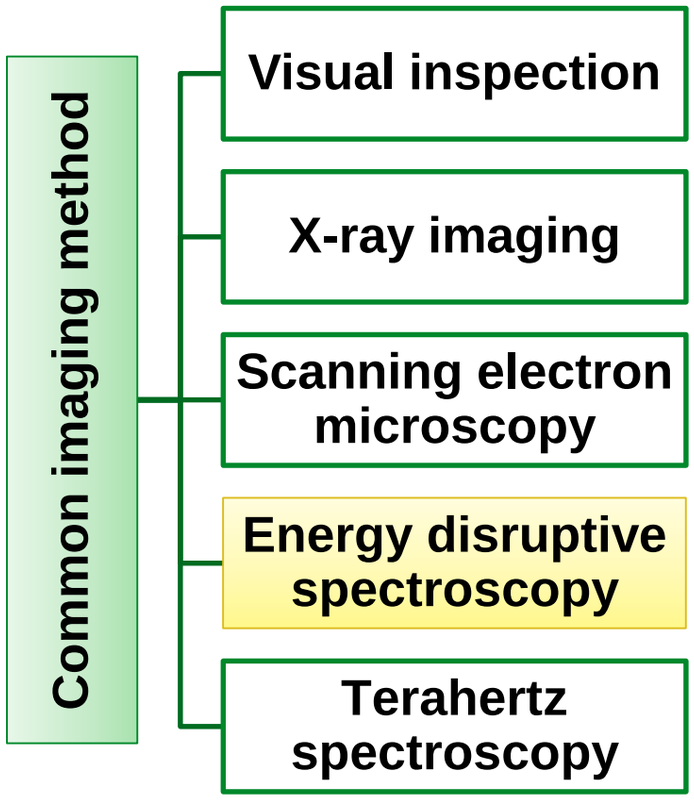


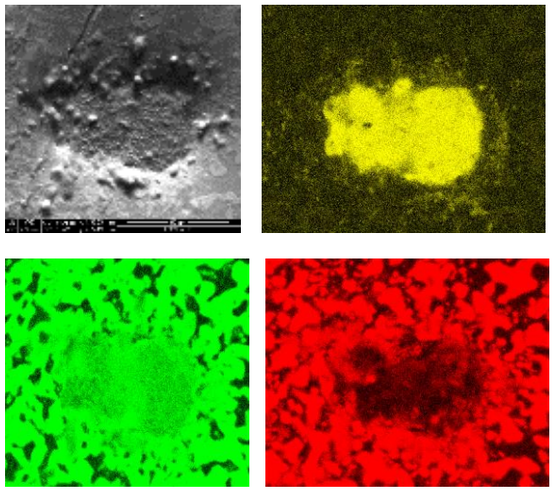
- Generates an image with a superfine resolution by using a focused electron beam moved across the sample surface
- Large depth of field makes it possible to keep surface features at radically different heights in focus simultaneously
  - 3D SEM imaging is also possible
- Ability to image at nanometer resolution allows for die inspection after decapsulation



Tilted (left and middle) and reconstructed 3D (right) images (Source: Shahbaz et al., ISTFA 2014)

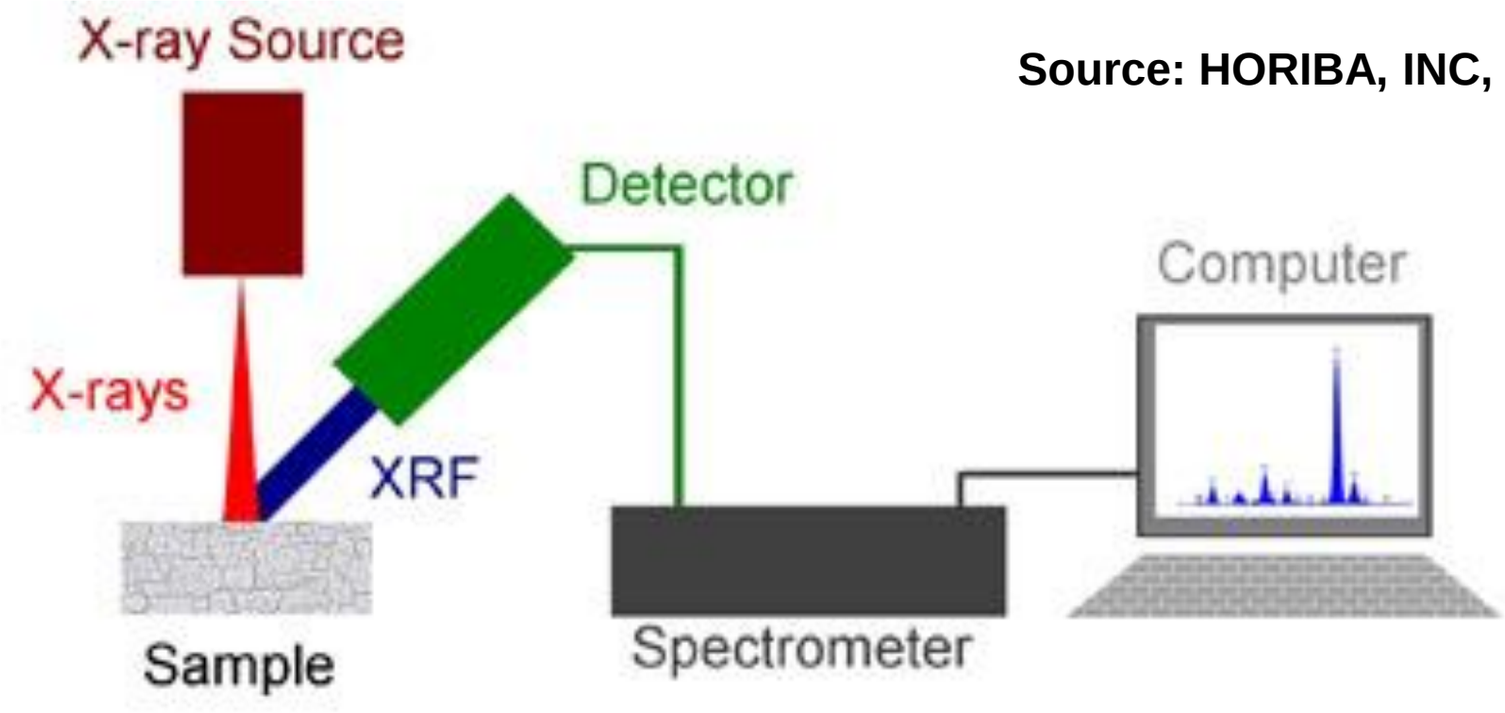
Energy Disruptive Spectroscopy (EDS)





Source: FICS Research

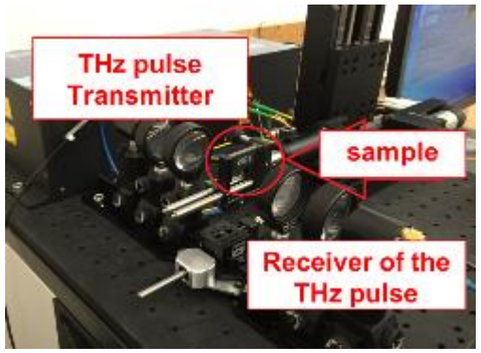
- Nondestructive method for material analysis
- High-energy X-rays cause outer electrons to reach unstable higher outer orbits and get collected by a detector
- Each element produces a unique peak in the spectrum



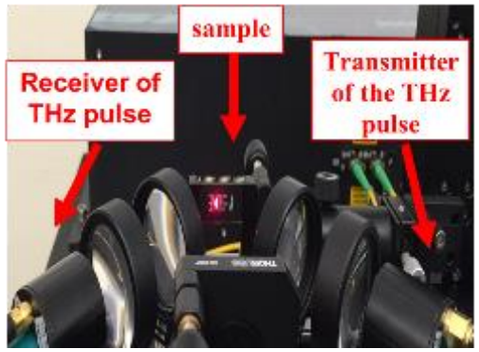
Source: HORIBA, INC,

Terahertz Time Domain Spectroscopy

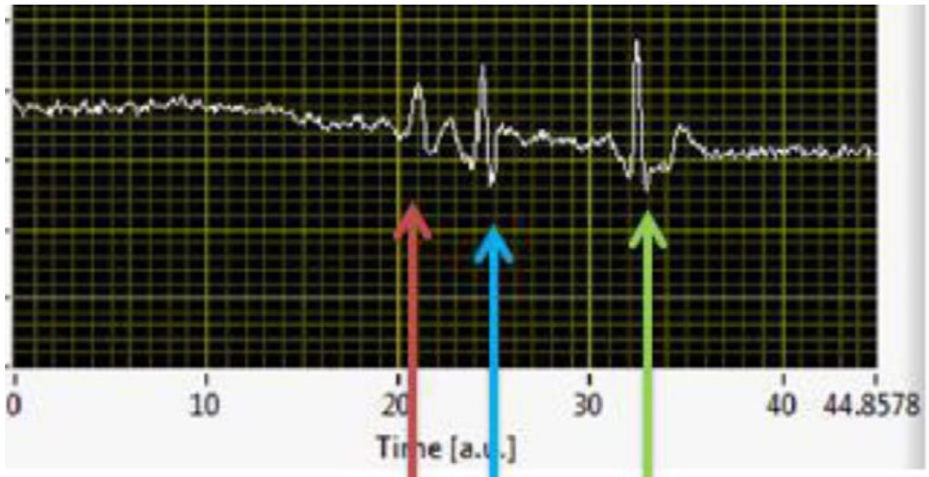
- Common imaging method
  - Visual inspection
  - X-ray imaging
  - Scanning electron microscopy
  - Energy disruptive spectroscopy
  - Terahertz spectroscopy

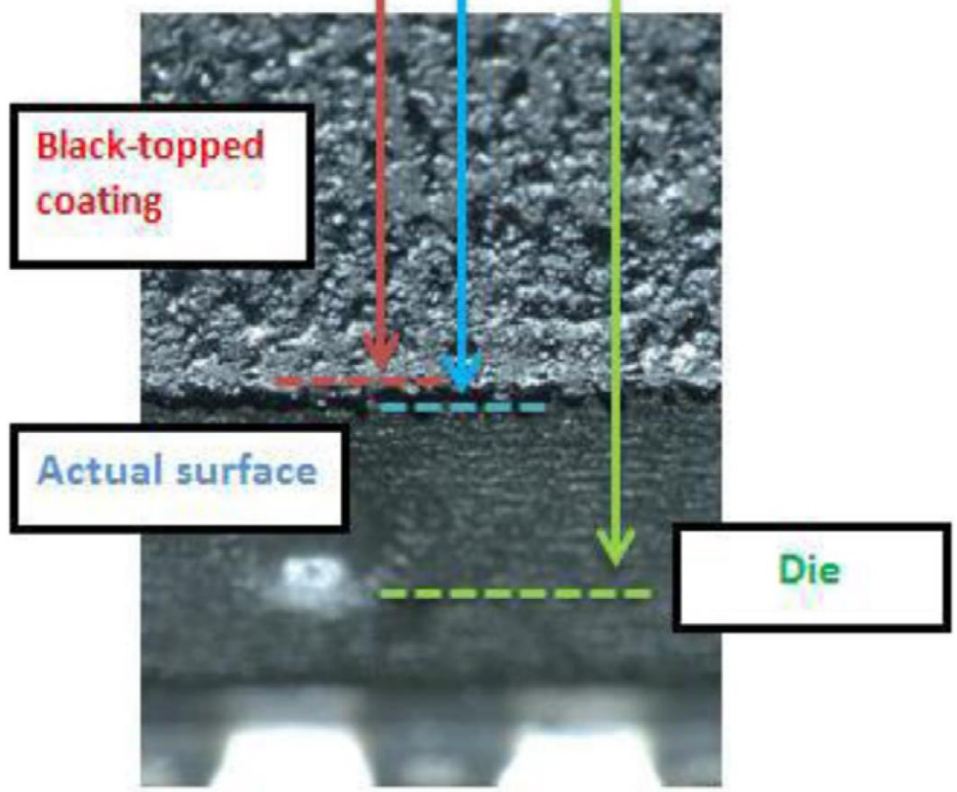


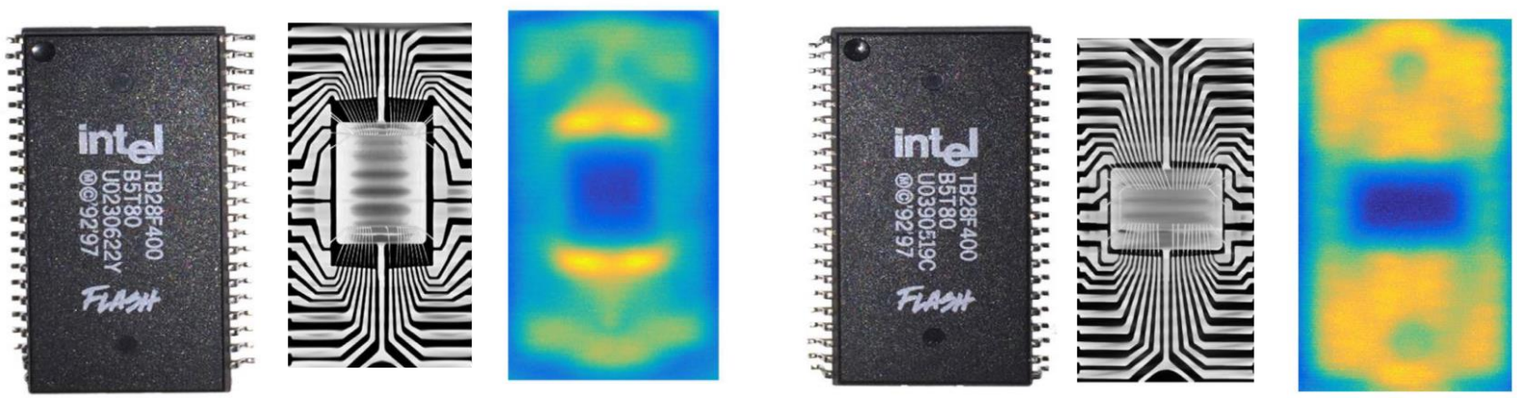
Transmission Mode (TM)



Reflection Mode (RM)







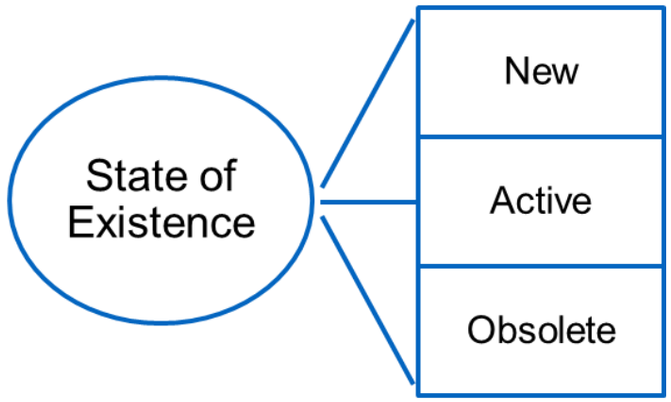
Optical, X-ray, and THz (TM) images from two Intel Flash with same lot marking, but clear differences in die orientation/lead frame

Source: Ahi et al, Opt Lasers Eng., 2018

Limitations of Physical Inspection

Counterfeit Types

- Recycled
- Remarked
- Overproduced
- Out-of-spec/Defective
- Cloned
- Forged Documentation
- Tampered

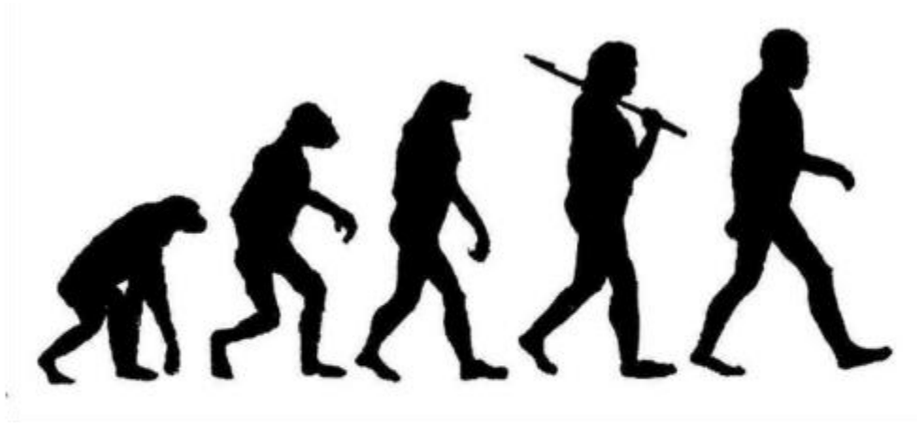


X-ray

SEM

FIB

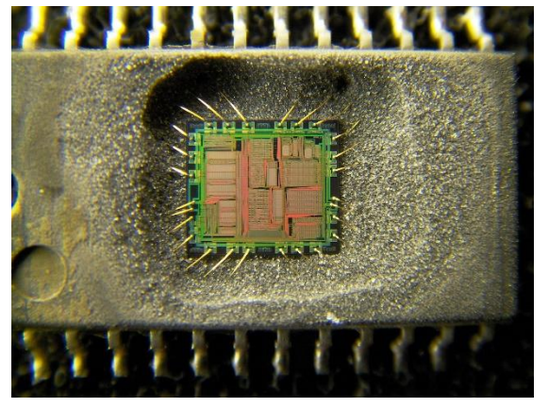
1. Diversity/Scope



3. Evolution and trends

4. Complete reliance on subject matter experts (SMEs)

2. Large test time and cost



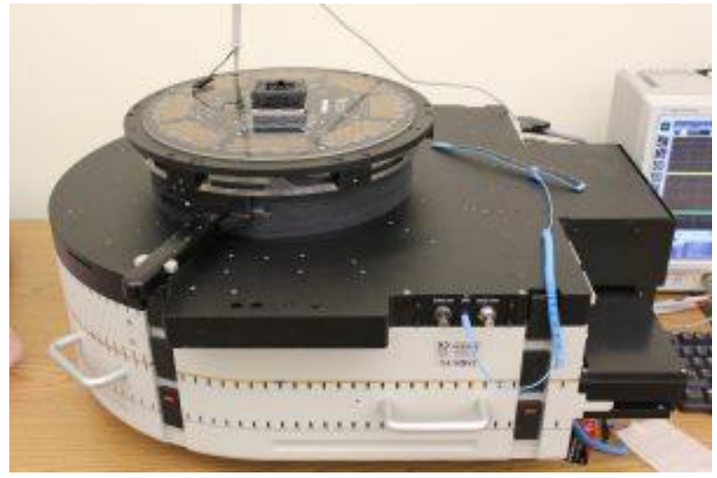
5. Destructive

Source: eenewsanalog.com

Electrical Defects and Tests

Advantages:

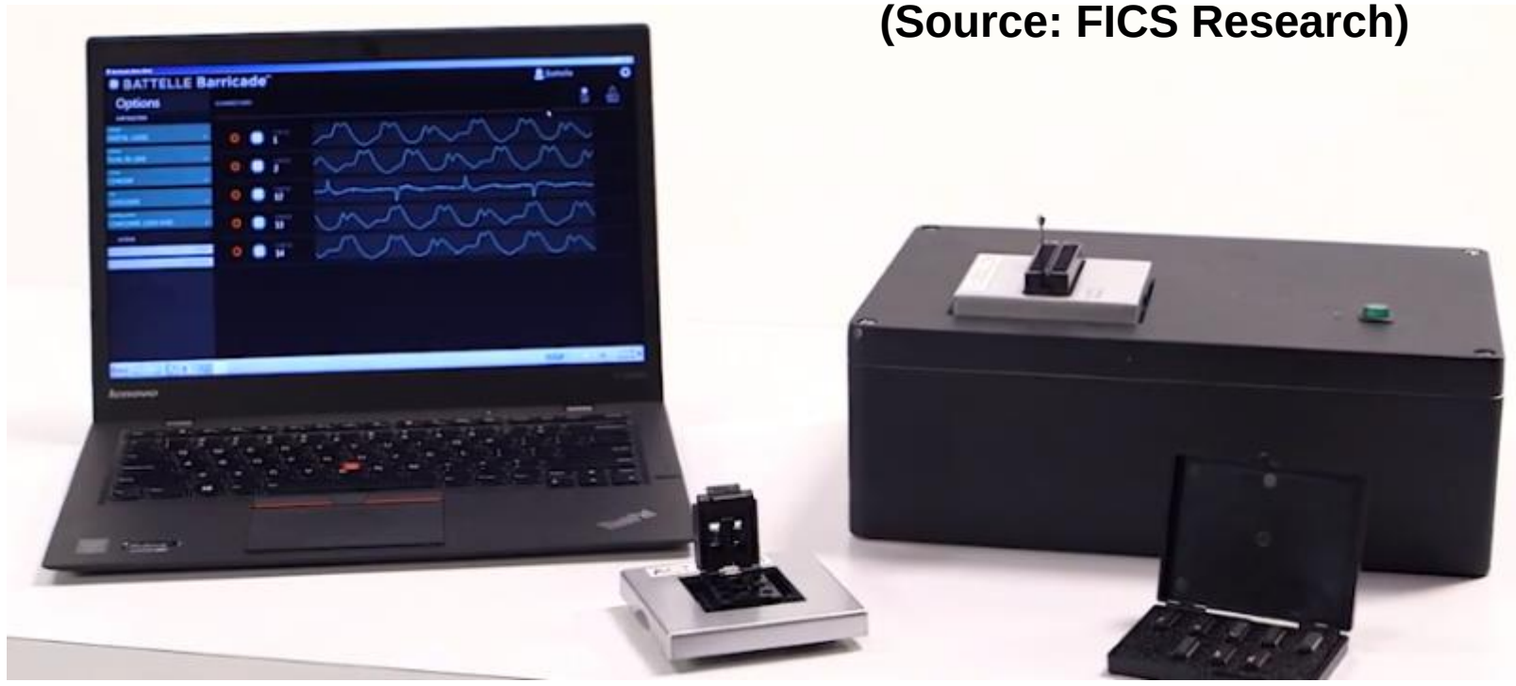
- Less expensive and time consuming than physical inspection
- Complementary to physical inspection (e.g., detect out-of-spec/defective and some clones)
- Can capture chip functionality



Invoys Ocelot-ZPF ATE (Source: FICS Research)

Test Equipment

- Standard testbench equipment
- Automatic Test Equipment (ATE)
- Commercial systems



Barricade System (Source: Battelle)

Curve Trace Tests

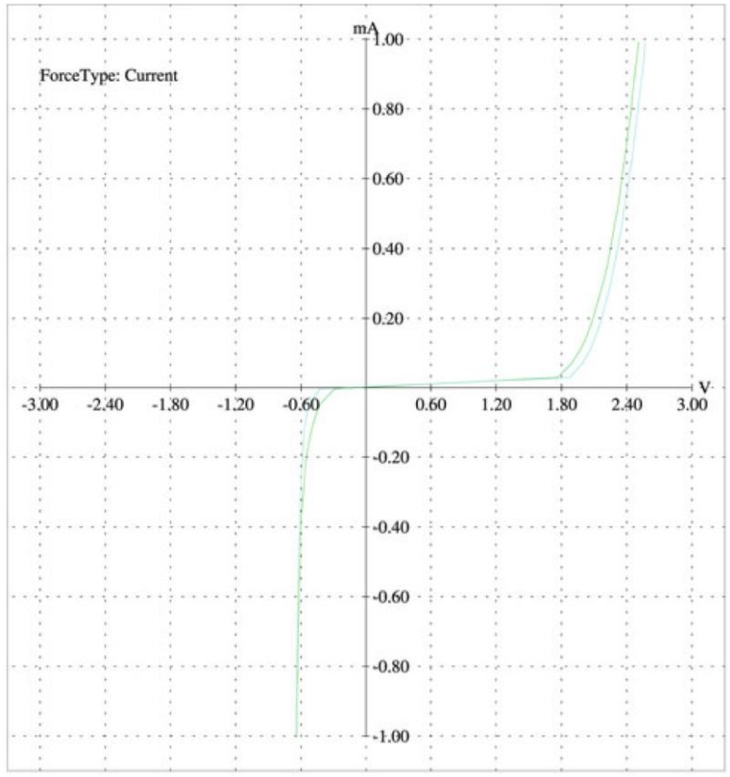
Test Types

- Basic (not powered)
- Powered

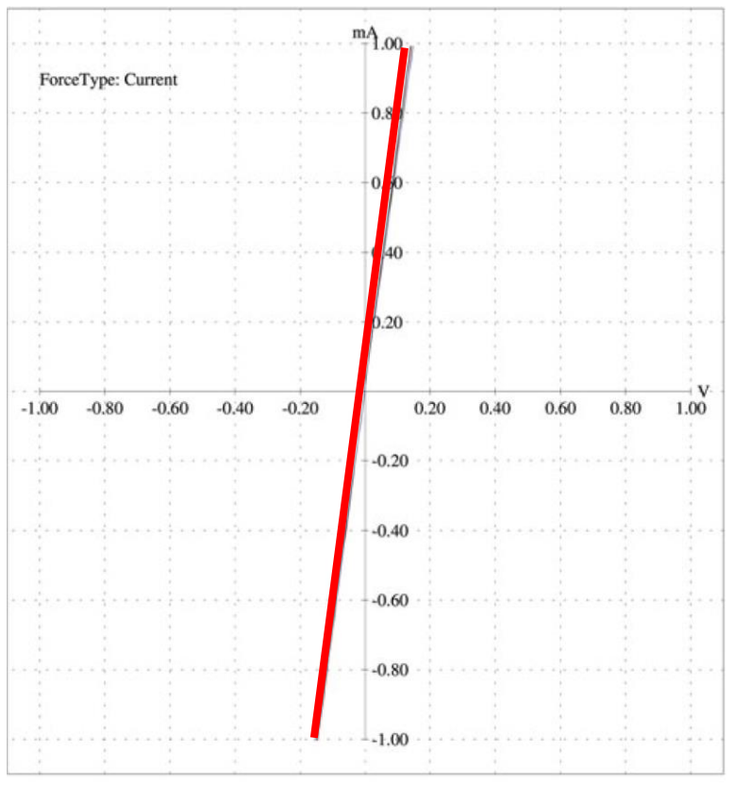
Pros

- Non-destructive
- No need for golden component
- Detect defects related to recycling
  - Package (e.g., damage to hermetic seal)
  - Missing, damaged, and broken bond wires
  - Missing, wrong, and cracked die

Curve Trace Pass



Curve Trace Fail



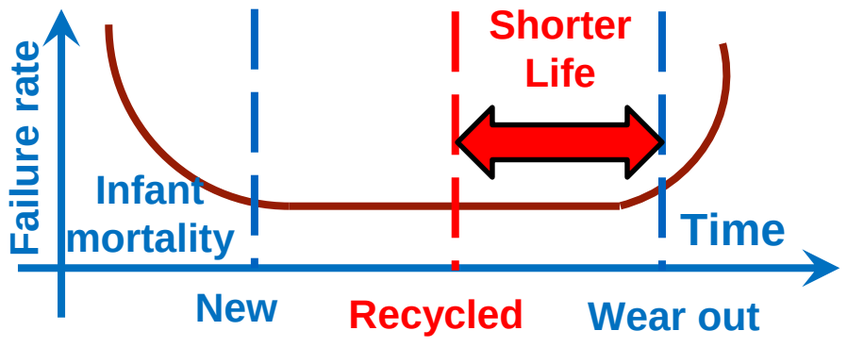
Source: Integra Technologies

Key Parameter Testing

- Similar to tests used for detecting defects after packaging by assembly
  - DC tests: contact test, power consumption test, etc.
  - AC tests: impedance, timing, etc. performed with AC voltages at different frequencies
  - Memory tests: voltage bumping, leakage, march, etc.
- Detects parametric defects
  - Threshold voltage variation, time-dependent dielectric breakdown (TDDB), resistive open/short, out-of-spec static or dynamic current leakage, thermal profile, delay profile
- **Pro:** Most effective way of verifying the functionality of a component
- **Cons:** Requires expensive test setup and development of complex test programs (if unavailable)

Burn-in Testing

- Component is operated at a stressed condition (high voltage and/or temperature) to accentuate infant mortality and other unexpected failures



Minimum temperature T_A(°C)	Minimum time (h)			Test condition[3]	Minimum reburn-in time (h)
	Class level S[1]	Class level B[2]	Class level S hybrids (Class K)		
100	—	352	700	Hybrids only	24
105	—	300	600	”	24
110	—	260	520	”	24
115	—	220	440	”	24
120	—	190	380	”	24
125	240	160	320	A–E	24
130	208	138	—	”	21
135	180	120	—	”	18
140	160	105	—	”	16
145	140	92	—	”	14
150	120	80	—	”	12
175	—	48	—	F	12
200	—	28	—	”	12
225	—	16	—	”	12
250	—	12	—	”	12

[1] High reliability military applications (Class level B).
[2] Space applications (Class level S).
[3] Test Conditions defined in Section 3.1 MIL-STD-883 [14]

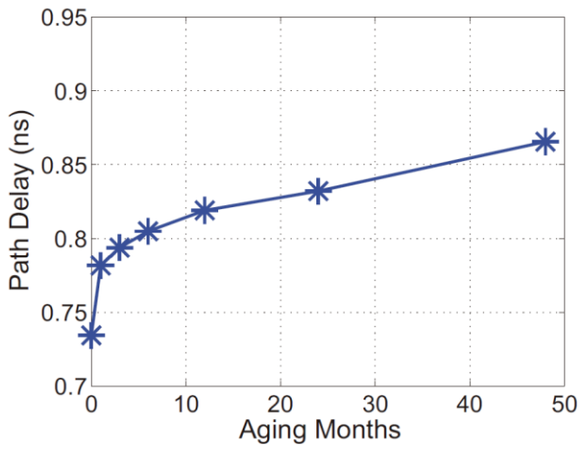
Source: Department of Defense, Test Method Standard: Microcircuits

- **Pro:** Detect latent defects
- **Con:** Partially destructive, i.e., months to years of device life are consumed

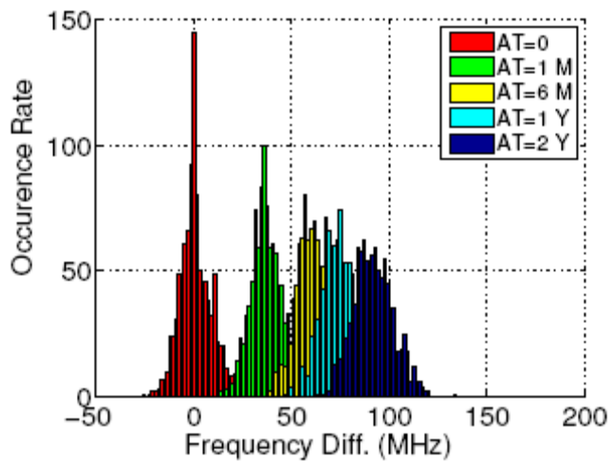
Aging Based Analysis

Path Delay Fingerprinting

- Due to degradation in the field, the path delay distribution of recycled ICs will become different compared to new ICs

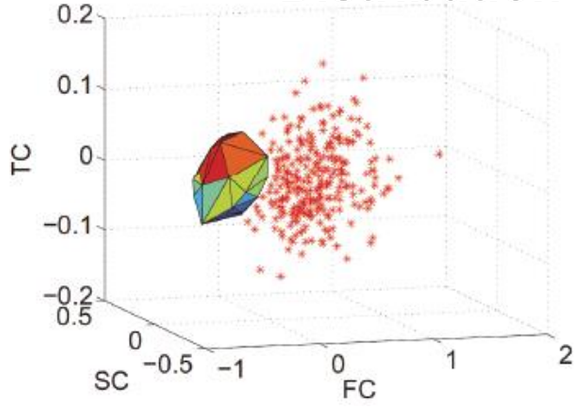


Degradation of a critical path



Path Delay Distribution

PCA results: 3 Months

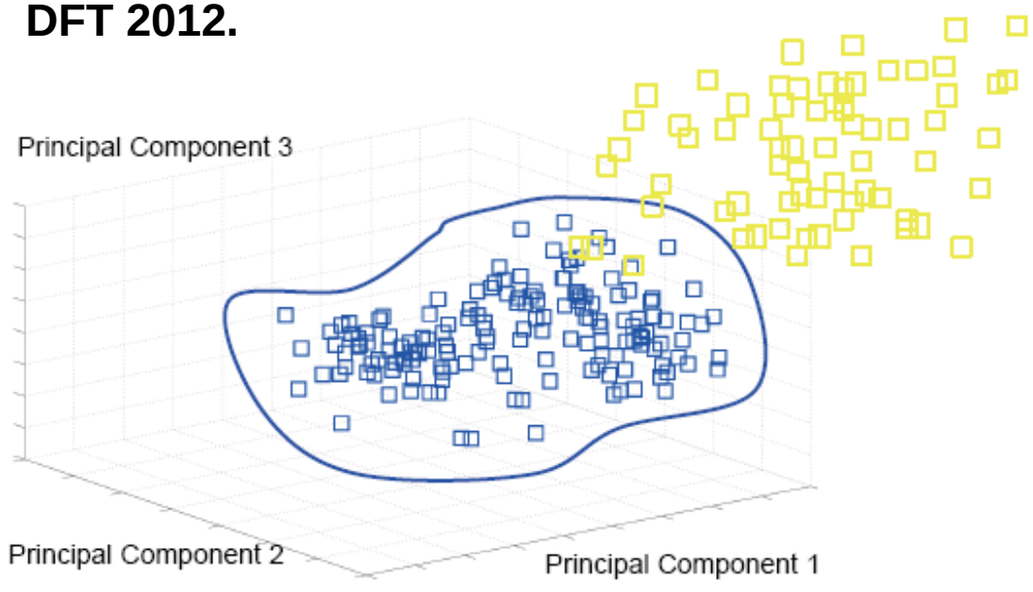


Source: Zhang et al, DFT 2012.

Early Failure Rate (EFR) Data Analysis

- Statistical approach (SVM) to detect recycled ICs
- Training a one-class classifier using only brand new devices

Source: Huang et al, DFT 2012.



Projection of devices at t = t_0; t_4, shown by blue and yellow squares, respectively.

Section IV: Advanced / Automated Physical Inspection

Counterfeit-IC.org

Current Content:

433 optical images from 113 sample chips of 23 different products (Intel, AMD, TI, Avago, Tundra, and more)

Planned Additions:

Over 1000 images from Intel and Tundra chips

A resource sponsored by the National Science Foundation (NSF) to

- **VIEW** and **EXPORT** images and statistical information related to counterfeit defects
- **UPLOAD** images of defects found by physical inspection of counterfeit ICs
- **DEVELOP** automated counterfeit IC detection techniques
- **LEARN** more about the defects found in counterfeit ICs and counterfeit IC detection

Recent Progress in Automation

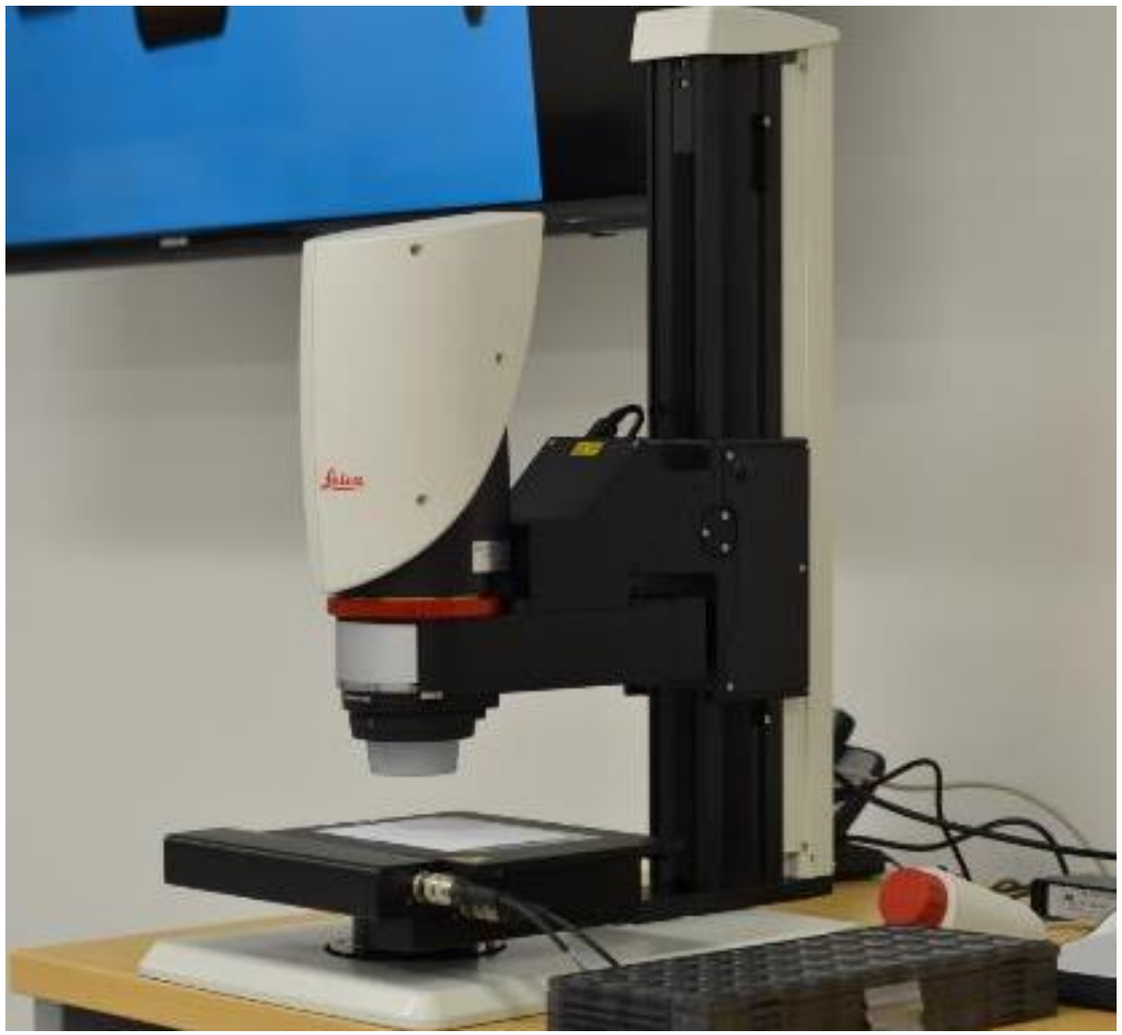
Goal: Make it easier to detect defects in IC chips, allowing for quicker identification of counterfeits

- Focused on marking displacements, texture differences and color variations thus far

Overview of Steps

1. Marking Selection: Identify markings of interest from reference chip image
2. Imaging: Capture high resolution images from chips under inspection
3. Registration: Align and rotate all chip images to match reference chip image
4. Displacement: Compute normalized cross-correlation to find markings in chip under inspection, calculate displacement, and annotate image
5. Texture Difference: Segment surface and classify rough vs. smooth surfaces via local binary patterns (LBP)
6. Color Variations: Compute color histogram and compare with reference to identify discolorations

Imaging Setup - Leica DVM6



- High resolution digital microscope with 16:1 zoom ratio
- Fully apochromatic corrected optics and a 10M pixel camera with fast live imaging mode
- Motorized stage has 3 degrees of freedom in x, y, and z direction which enables automatic stitching and 3D surface imaging
- ‘Mark and Find’ software defines multiple stage locations and revisits them automatically

Registration

Pre-processing Step

- To correctly orient all the images, a “reference” image of an ideal chip was used
- For example, the reference image and an actual data image are shown on the next slide

Reference Image

Image to be Registered

Initial Registration Approach

- To ensure the accuracy of defect identification, it is important to have all the images in the same orientation and XY positioning
- Registering all the images allows mark, texture and color comparisons to be more accurate, as there ideally wouldn't be external factors like relative position affecting any of the comparisons

MATLAB's Built-in Registration Function

- Rotated but didn't perform translation well
- Applying Gaussian filter to blur out marking features and reduce miscalculations
- Binarized images, but too much important information was lost

Finally started looking at Hough transforms to identify lines/edges in the image

Custom Registration Algorithm

1. Depending on the region of chip in question, 1/10th of the image where the edges might be located are analyzed
2. Canny edge detection is used to identify all the possible edges in the subimages
3. Hough transforms are used to identify the major/important edges in the image (based on threshold values)

Original Image

Binarized Image

Edge Detection

Custom Registration Algorithm

4. The orientation of the edges can be calculated, and the entire image is rotated to make the edges parallel to the XY axes
5. A displacement transformation matrix is added to align the current image's edges with the reference image's edges
6. Fill in black spaces with information from the reference image (usually just edge pixels)

Rotated Image

Shifted Image

Final Registered Image

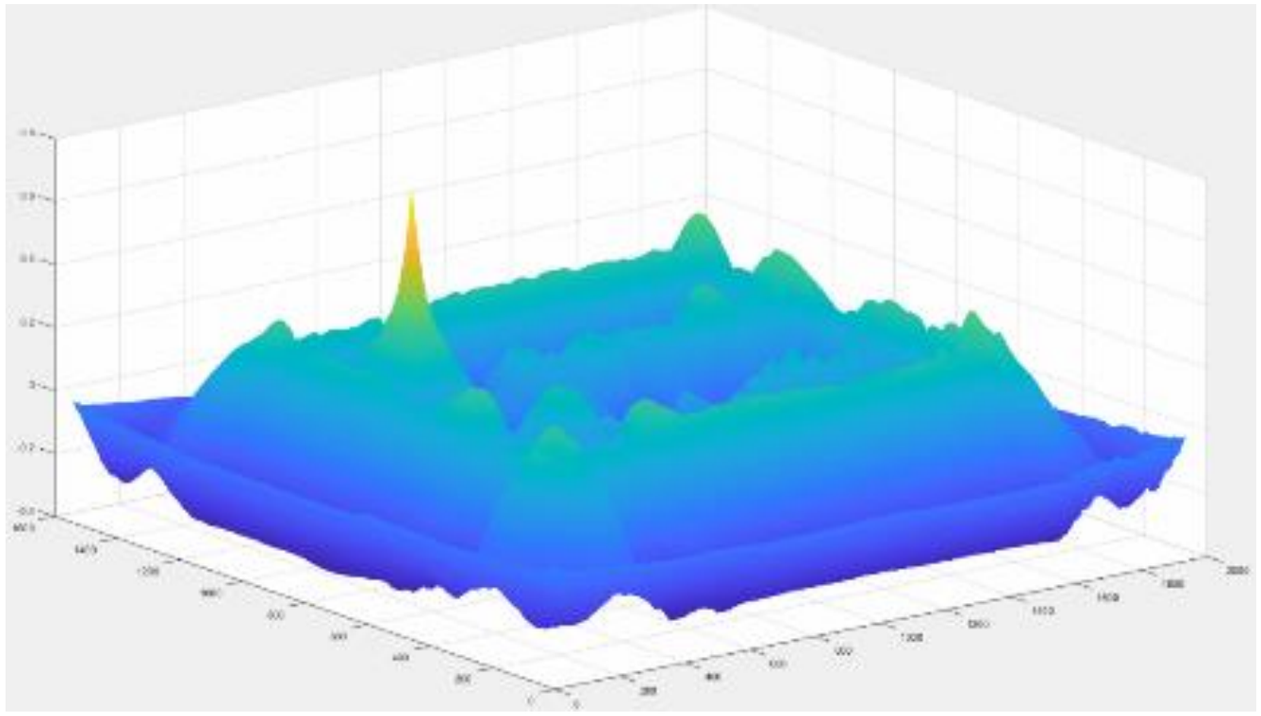
Marking Displacement

- By registering the images, the comparisons necessary to measure the displacement of identification markings became a lot easier to perform
- The algorithm works by first allowing the user to identify the markings of interest on the reference images

Image Marked by User

Normalized Cross Correlation Function

- Using a normalized cross correlation function, the sub-images created by the user are compared to each data image to generate a 3D surface
- The 3D surface returned the correlation values for every possible positioning of the sub-image over the data image
- The highest correlation value corresponds to the location of that corresponding marking on chip in question

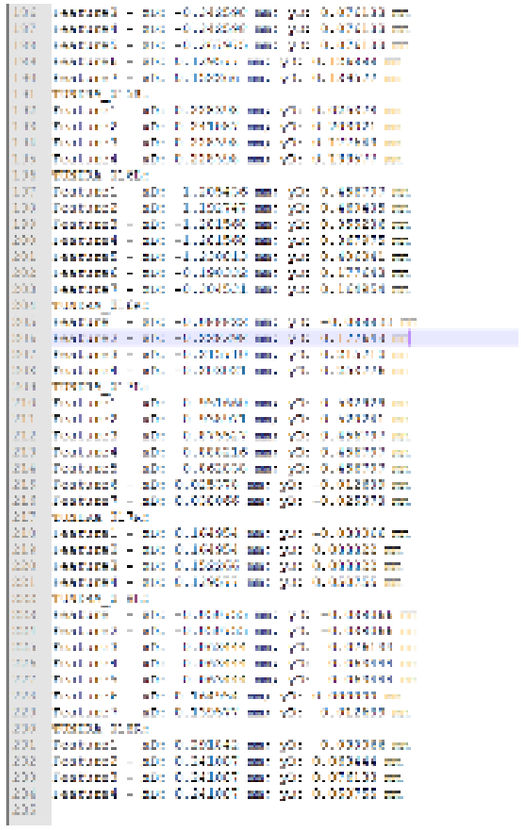


3D Correlation Surface

- The peak's location is found, and compared to the corresponding location on the reference images
- The difference is calculated and converted to millimeters using a pixel-to-millimeter ratio determined when the pictures were obtained

Marking Displacement Outputs

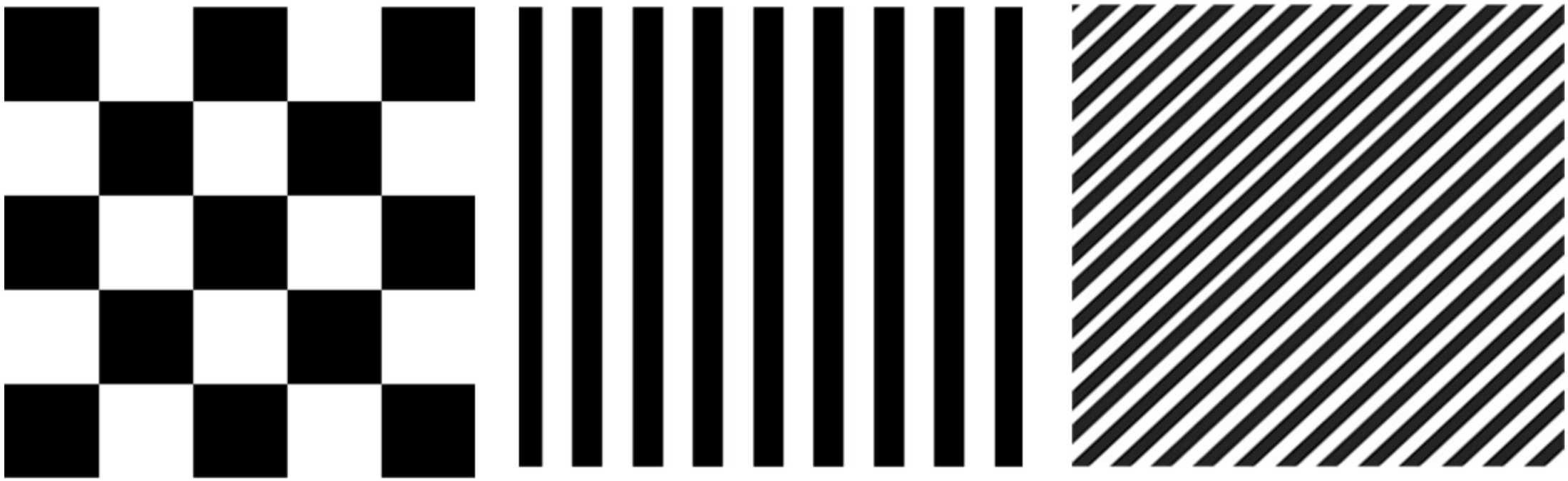
- All the results are stored in a text file for the user to peruse later
- Additionally, new images are returned with the marking displacements clearly identified



Displacement Text File

Annotated Displacements

Package Texture based Detection



(a) Checkerbox (b) Vertical stripe (c) Horizontal stripe

“Texture” is the spatial distribution pattern of pixel intensities
A non-counterfeit IC package is expected to have identical texture over its surface, while for a counterfeit sample, there is possibility of texture being different, either on the same surface, or the surfaces of different samples from the same lot.

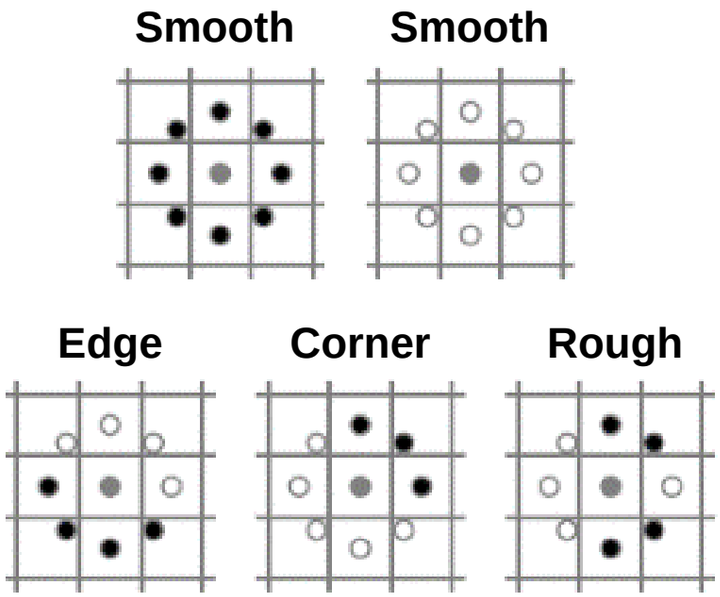
Local Binary Patterns

A technique called LBP, or Local Binary Patterns, was used to analyze and classify the texture of regions

1	2	7
9	5	6
1	3	5

≥ 5 →

0	0	1
1		1
0	0	1



Laws' Texture Energy Features

This "texture-energy" approach measures the amount of variation within a fixed-size window (a typical window size is 15x15). In this method, four vectors are used to form nine convolution masks. Each of the vectors are chosen to detect particular features.

- **L5 (Level) = [1 4 6 4 1]^T**
- **E5 (Edge) = [-1 -2 0 2 1]^T**
- **S5 (Spot) = [-1 0 2 0 -1]^T**
- **R5 (Ripple) = [1 -4 6 -4 1]^T**

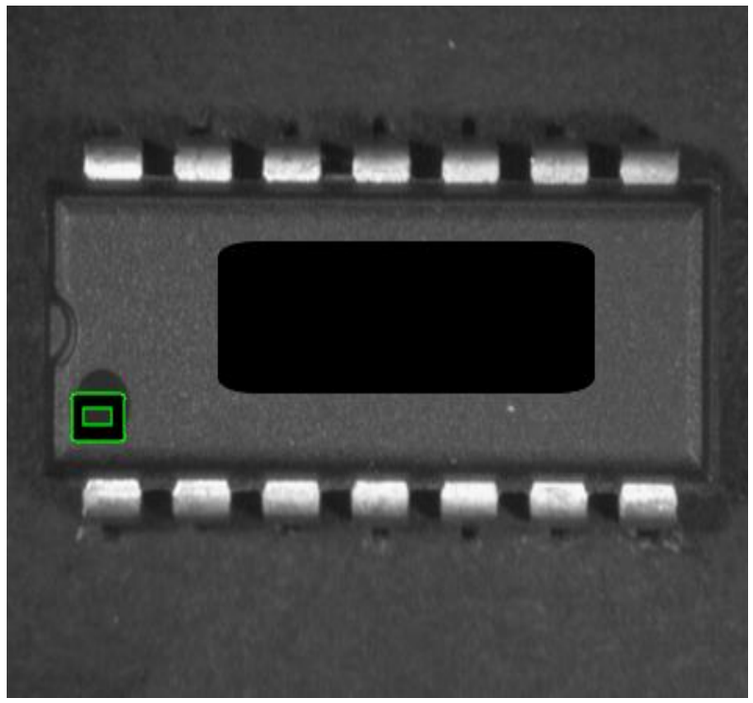
Symmetric pairs are combined to produce following nine convolution mask by taking the outer product of the vectors:

(L5E5^T+E5L5^T)	**(L5S5^T+S5L5^T)**	**(L5R5^T+R5L5^T)**
(E5S5^T+S5E5^T)	**(E5E5^T)**	**(E5R5^T+R5E5^T)**
(S5R5^T+R5S5^T)	**(S5S5^T)**	**(R5R5^T)**

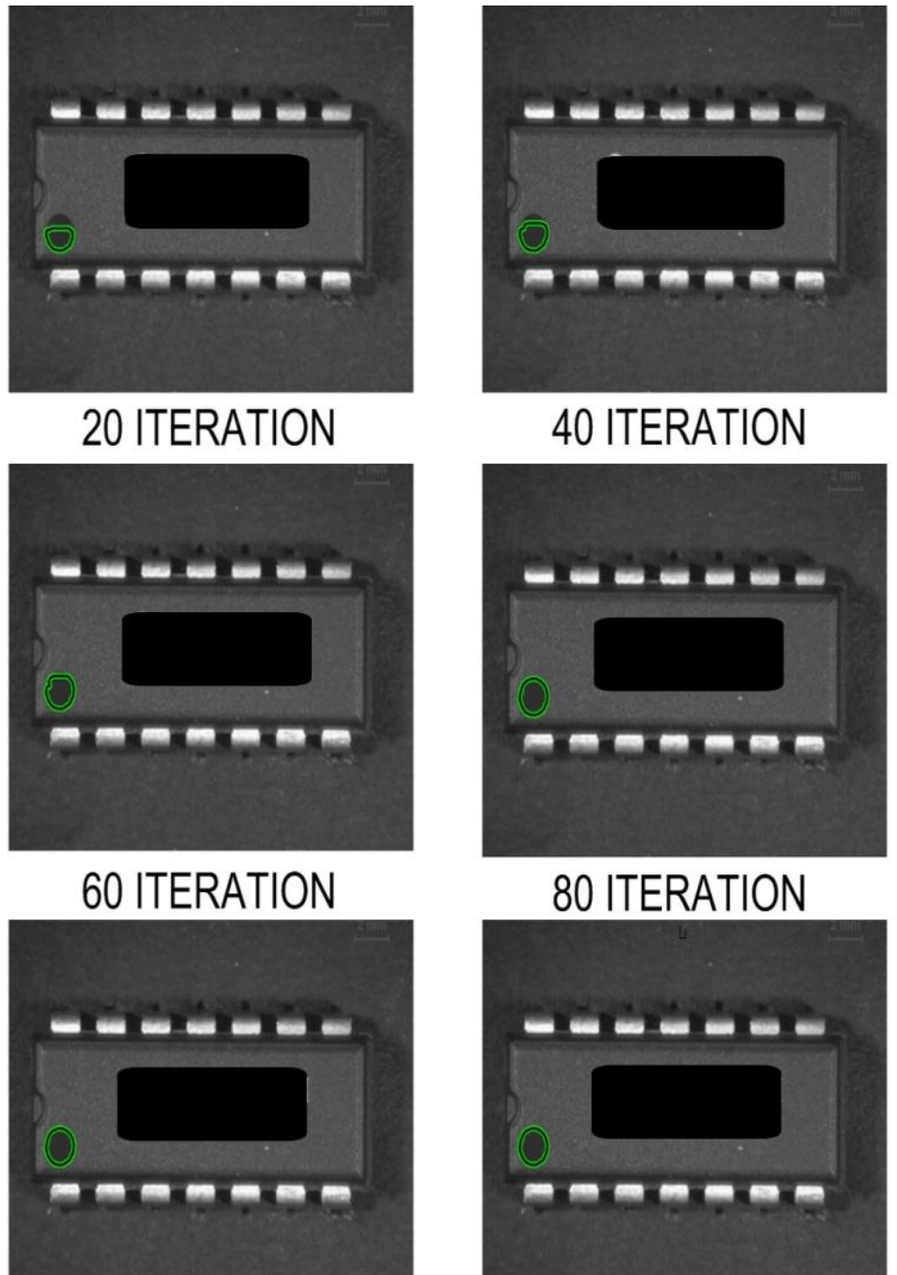
Package Indent Analysis

Analysis of IC Package indent is done by locating, measuring and comparing the indents present on IC surface.

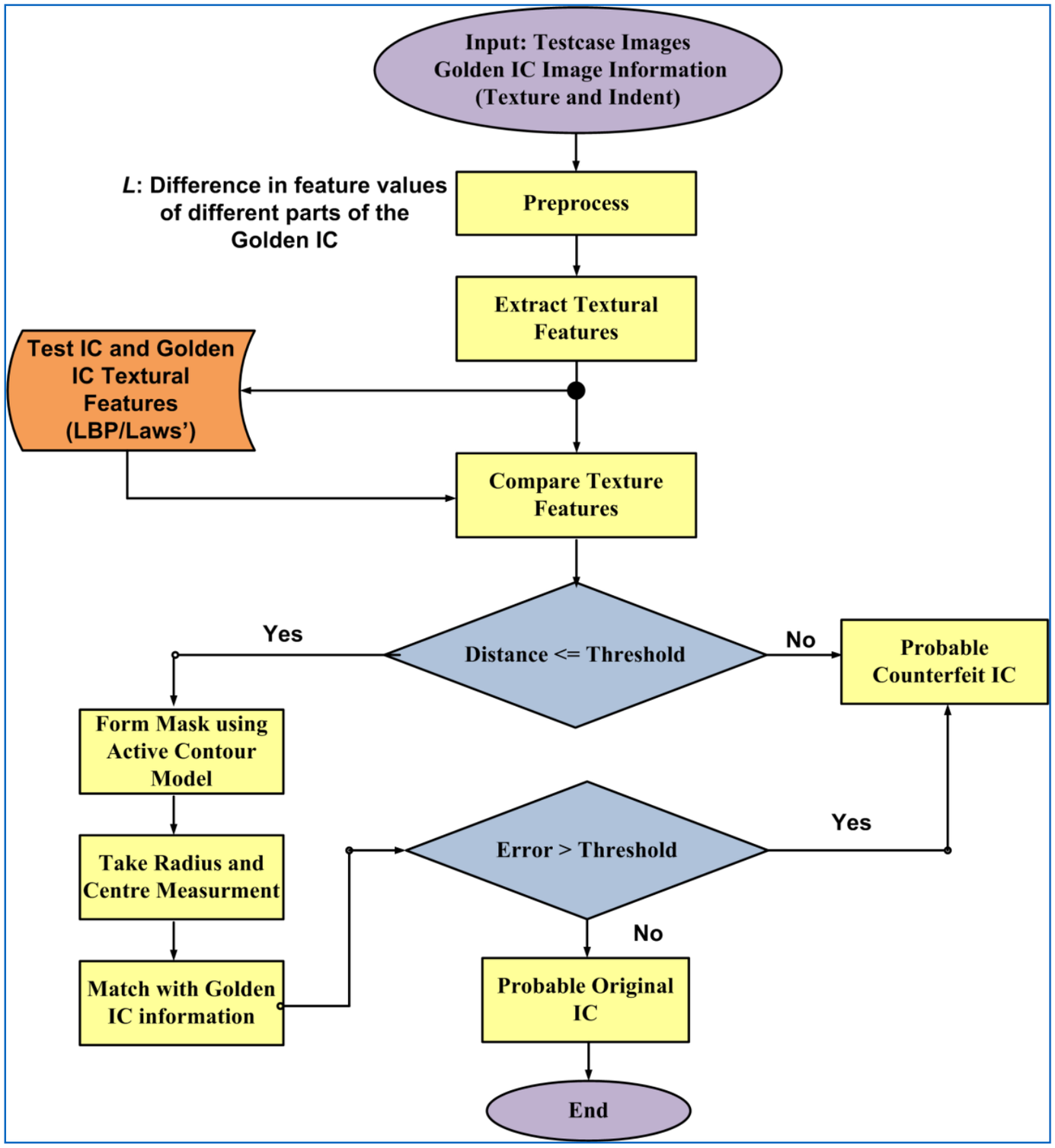
The main algorithm used for such analysis is *Active Contour Method*.



Initial Mask



Two-step Methodology



A two-step methodology combining texture comparison and and indent comparison helps to improve the detection accuracy, than only texture based detection

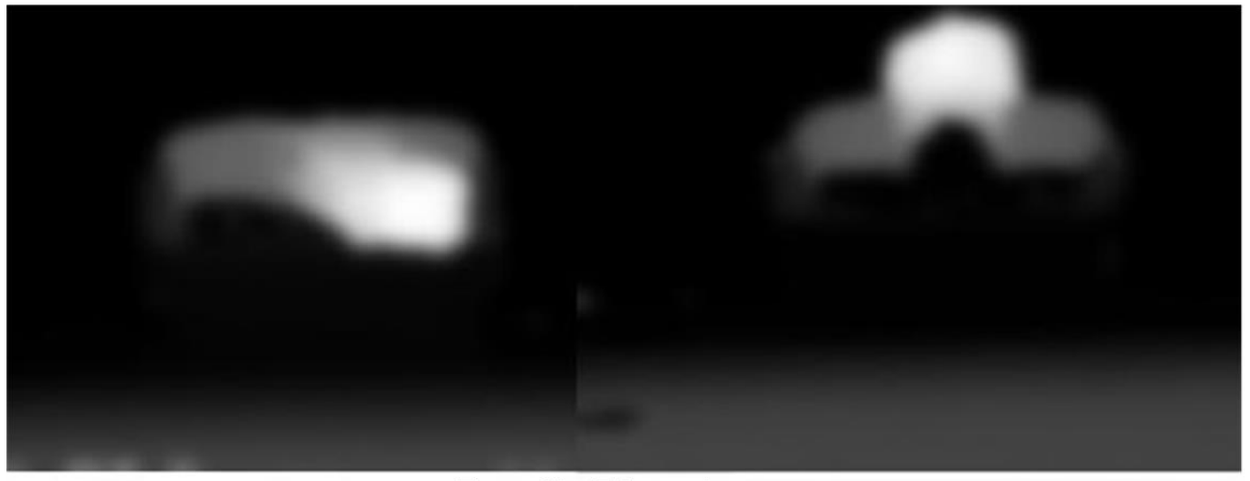
[Ghosh and Chakraborty, *IEEE TII*, 2018].

Unsupervised clustering technique (e.g. DBSCAN) can be used to further validate the results.

Sometimes, unsupervised techniques might be the only option.

IC Pin Image Analysis based Detection

- Detection of defective pins of ICs is done by identifying two types of defects commonly found in counterfeit ICs:
  - Bent Pin
  - Corroded Pin

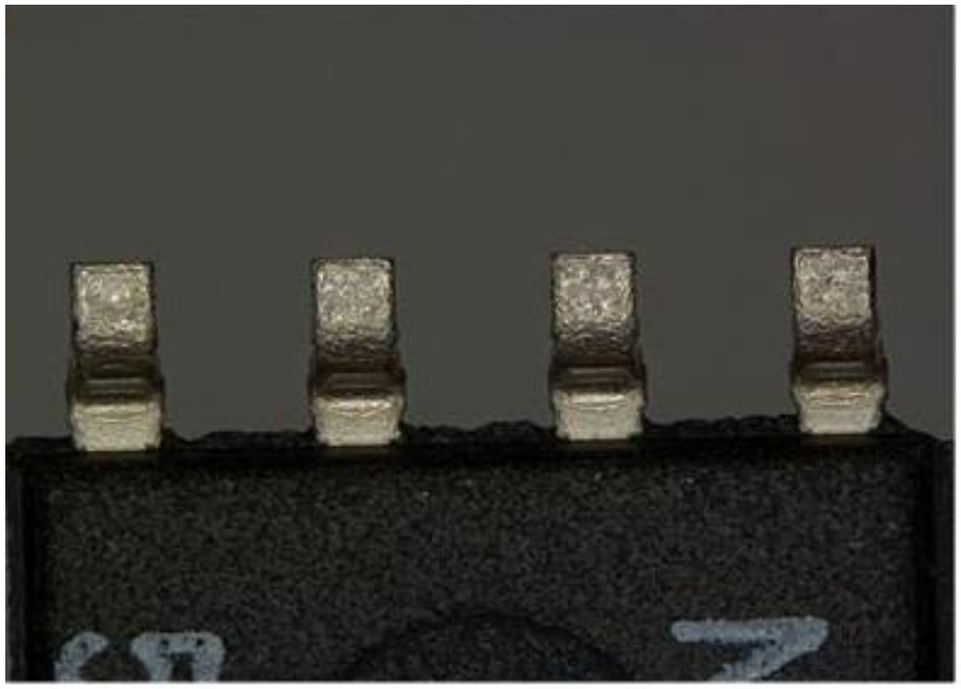


(a) Bent Pin **Depth Map Images** (b) Straight Pin

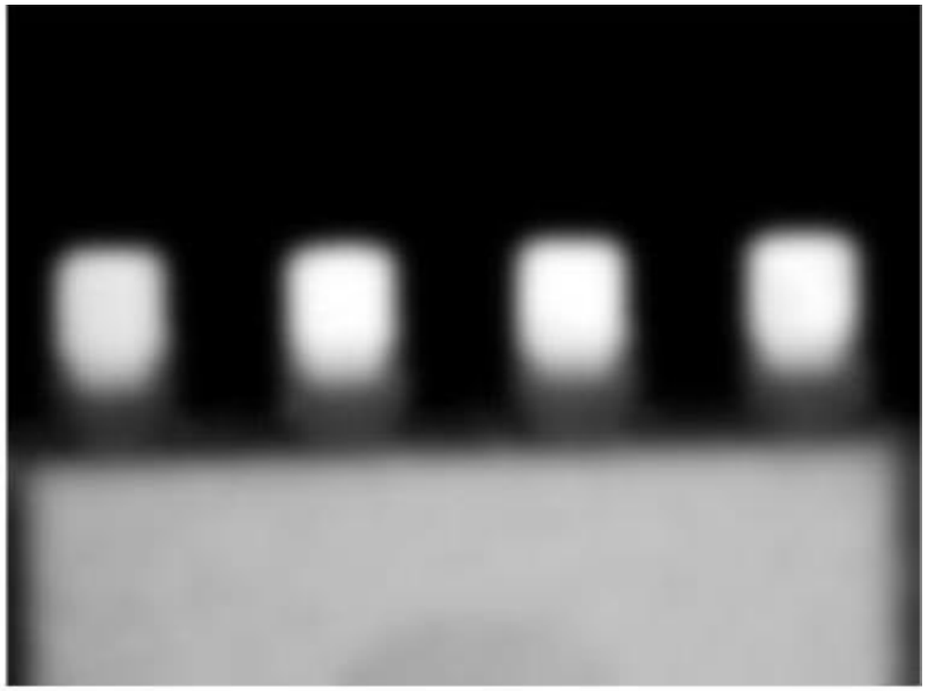
Side View Images

(c) Corroded Pin (d) Uncorroded Pin

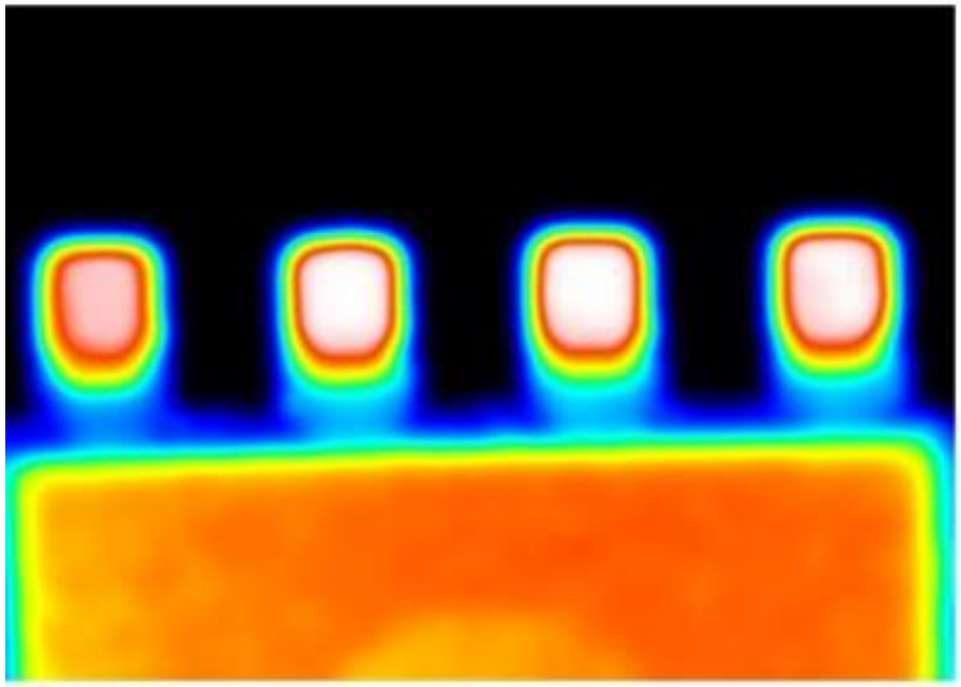
Examples of Depth Map Images



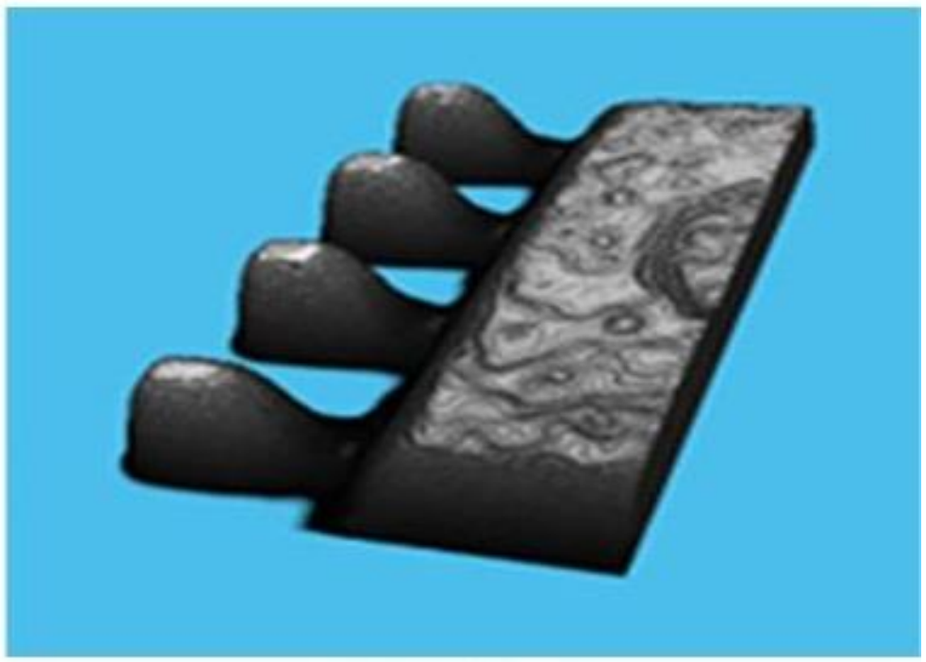
A: 2D image of part of an IC



B: Depth Map Image of A



C: Topographic Map of B



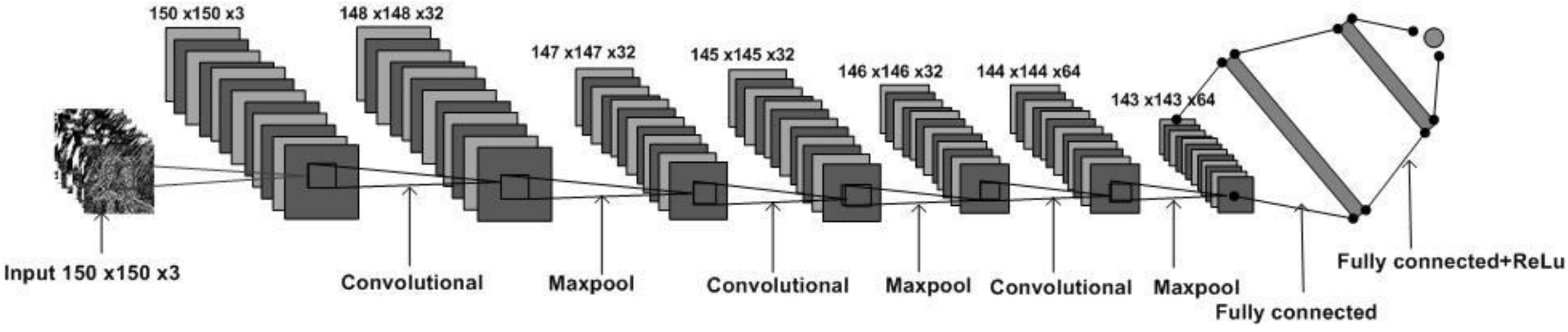
D: 3D Image of A

Supervised Techniques for Bent/Corroded Pin Detection

- **Support Vector Machine (SVM), K-Nearest Neighbour (KNN), Convolutional Neural Network (CNN)**

- **Dataset 1: This consists of 163 side-view images of individual IC pins, used for identification of ICs based on corroded pins. From this dataset:**
  - **For the SVM classier, five-fold cross-validation was implemented by dividing the dataset into 80% portion for training and 20% for validation associated with it.**
  - **For the KNN classier, four-fold cross-validation was implemented by dividing the data was divided into 75% portion for training and 25% for validation.**
  - **For the CNN classier, a subset of 131 images (74 images of corroded pins, and 57 images of undamaged pins) were used for training the classifiers, while a different subset of 32 images (18 images of corroded pins and 14 images of undamaged pins) was used for validation.**
- **Dataset 2: This consists of 144 depth map images of individual IC pins. For SVM and KNN classier design, dataset division as done for Dataset-1 was repeated, while for CNN, the training set consists of 114 images (57 depth map images of bent pins, and 57 depth map images of straight pins), and the validation set consists of 30 images (15 depth map images of bent pins and 15 depth map images of straight pins).**
- **Dataset 3: This consists of a subset of 90 depth map pins out of 144 depth map images of Dataset 2. This is used for only unsupervised bent pin detection.**

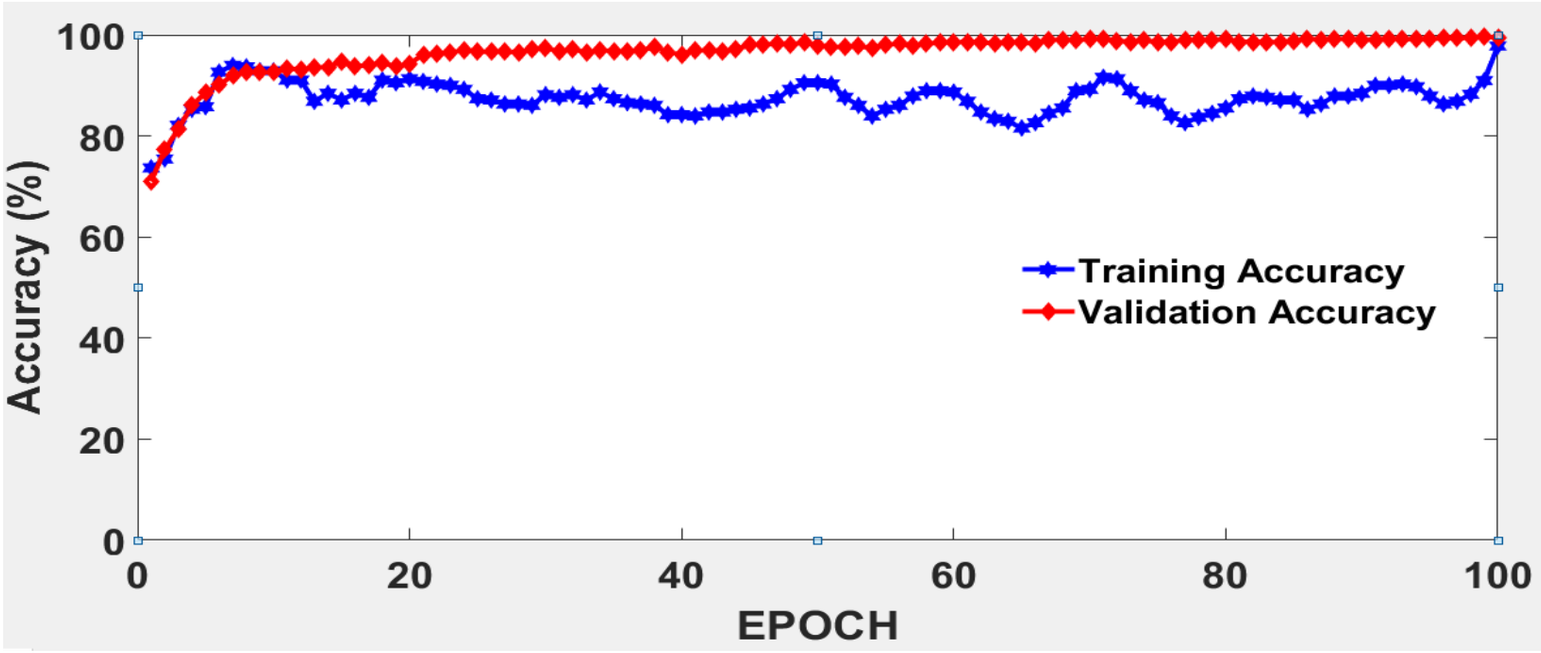
CNN Architecture Used



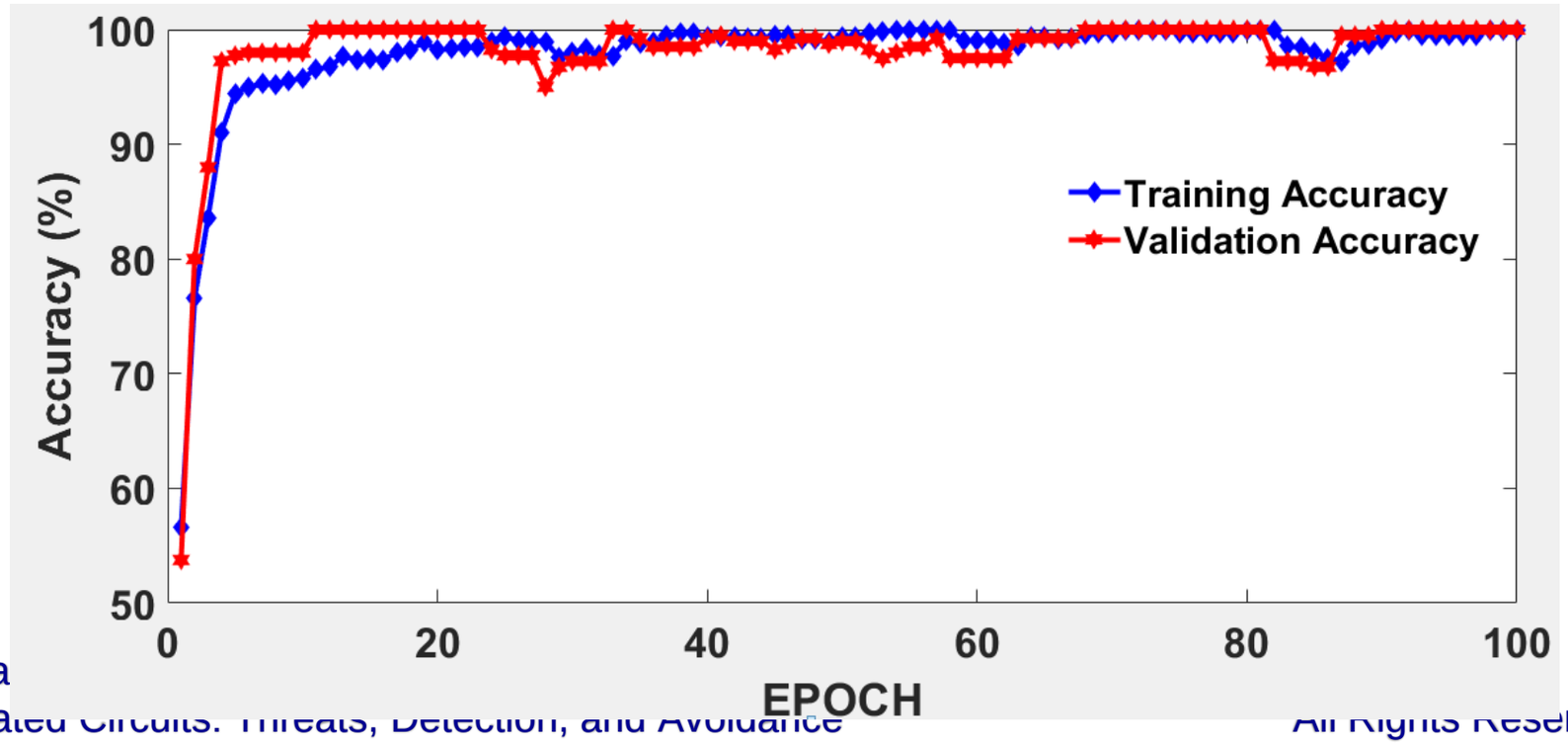
- **Architecture derived by trial-and-error from similar architectures previously found to be successful for image classification**
- **Raw image pixel values were used as the input**
- **No need for careful feature engineering (as required in the previous two approaches)**

CNN Detection Results

- **Bent Pin Detection**



- **Corroded Pin Detection**



Future Work

- Further improvements can be made to the discolorations detector
  - Improve adaptability by accounting for variances caused by different lighting
  - Implement a “color concentration” detector i.e. only identify locations with a larger concentration of the color in question rather than issues caused by a general spread
- Currently implementing an intelligent scratch detector
  - Training it to detect scratches regardless of orientation or clarity
  - Important to distinguish from markings
- **Importantly, unsupervised techniques need to be developed**

Section V: Counterfeit Avoidance Approaches

Counterfeit Avoidance

	Recycled	Remarked	Overproduced	Out-of-Spec/ Defective	Cloned
Digital & Small		**SHIELD**, ECID*			**SHIELD**, DNA, NR
Transistors, Diodes, and Passive Parts		**SHIELD**, DNA, NR			
Digital & Large — Programmable Logic ICs	**CDIR***	**SHIELD**, **PUF***, **HM***, **SST***, ECID*, DNA, NR	**HM***, **SST***	**SST***	**PUF***, **HM***, **SST***, NR, DNA
Digital & Large — Memory ICs					
Digital & Large — Microprocessor ICs					
Analog & Mixed Signal ICs		**SHIELD**, DNA, NR			**SHIELD**, DNA, NR

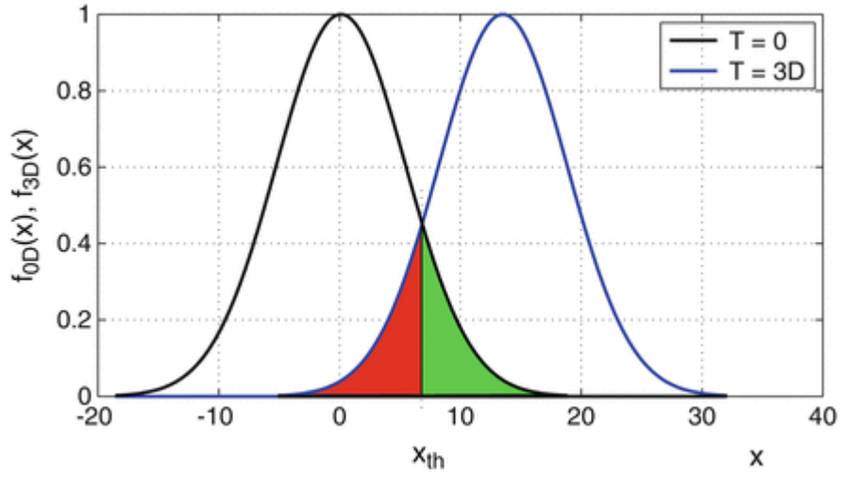
*** Only applicable to new chips and systems**

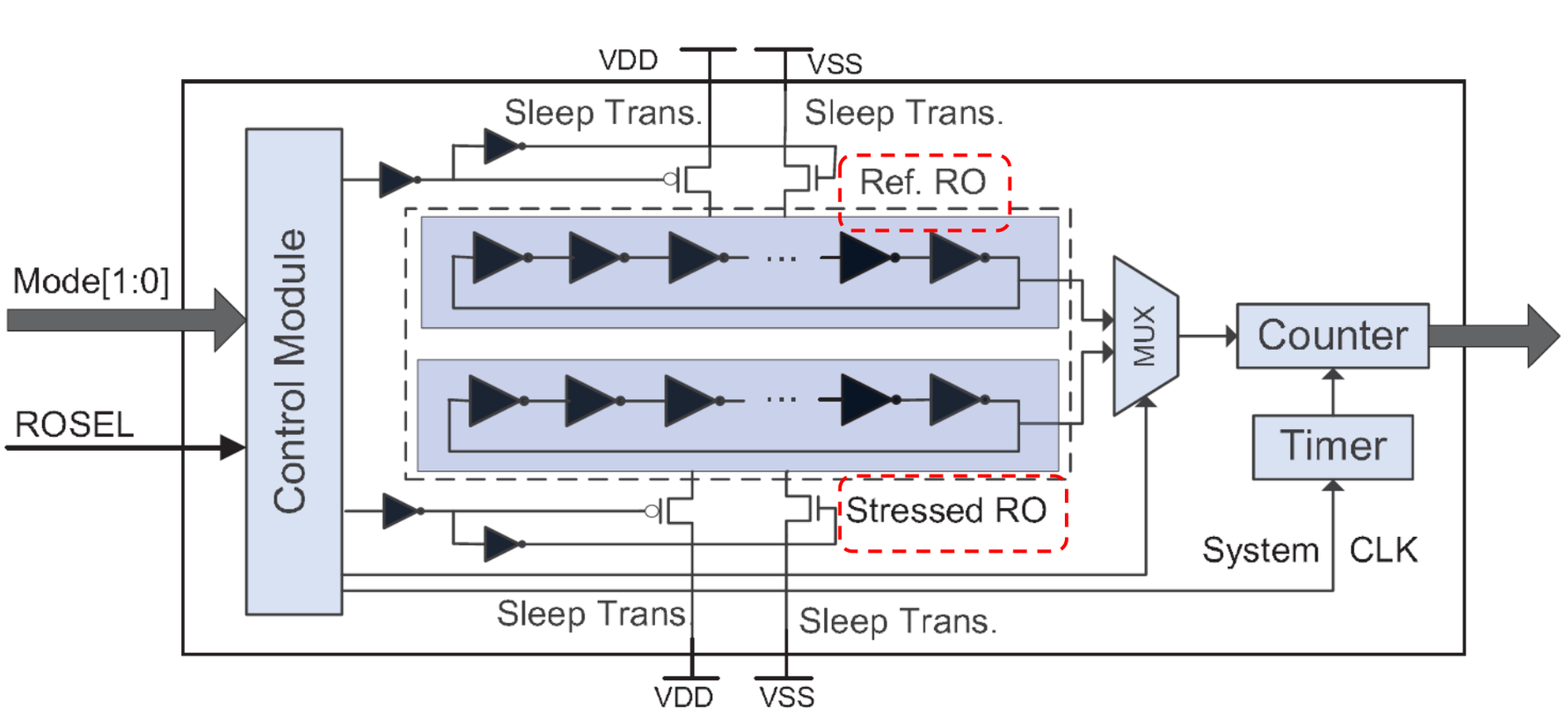
Combating Die/IC Recycling (CDIR)

- Composed of Reference RO and Stressed RO
- “Self-referencing” detection

Modes of Operation

- **Test:** Ref. RO and Stressed RO both off
- **Function:** Ref. RO off, Stressed RO is on
- **Measurement:** RO and Stressed RO both on





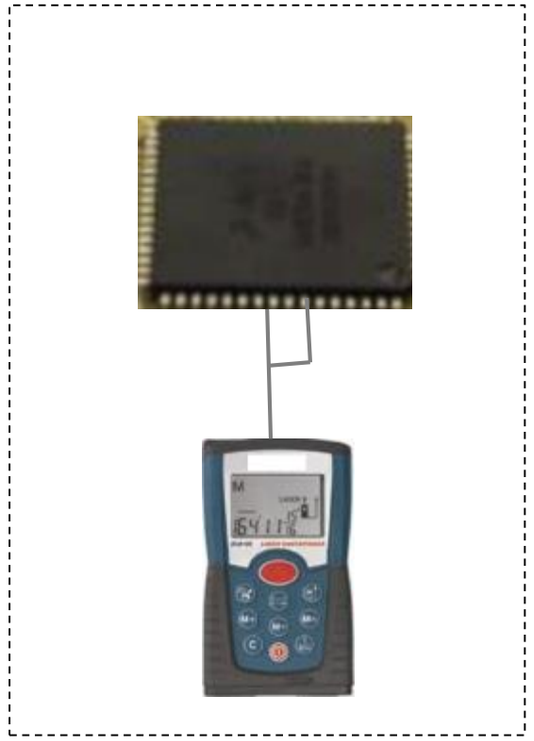


Image: Google

Source: Zhang et al, TVLSI 2013.

Who are the Cloners?

- Amateurs, small companies, and **state-funded** organizations
- Cloners in some countries argue that they don't trust U.S. manufacturers, so they clone U.S. chips to make sure their chips are free of hardware Trojans

Examples of Chinese Military's Copycat Culture (Source: USNI News)

Aircraft

Chinese Shenyang J-15 Flying Shark based on the Russian Sukhoi Su-33

Ground

AM General HMMWV Humvee Light Truck (U.S.) and Chinese Dongfeng EQ2050 Brave Soldier

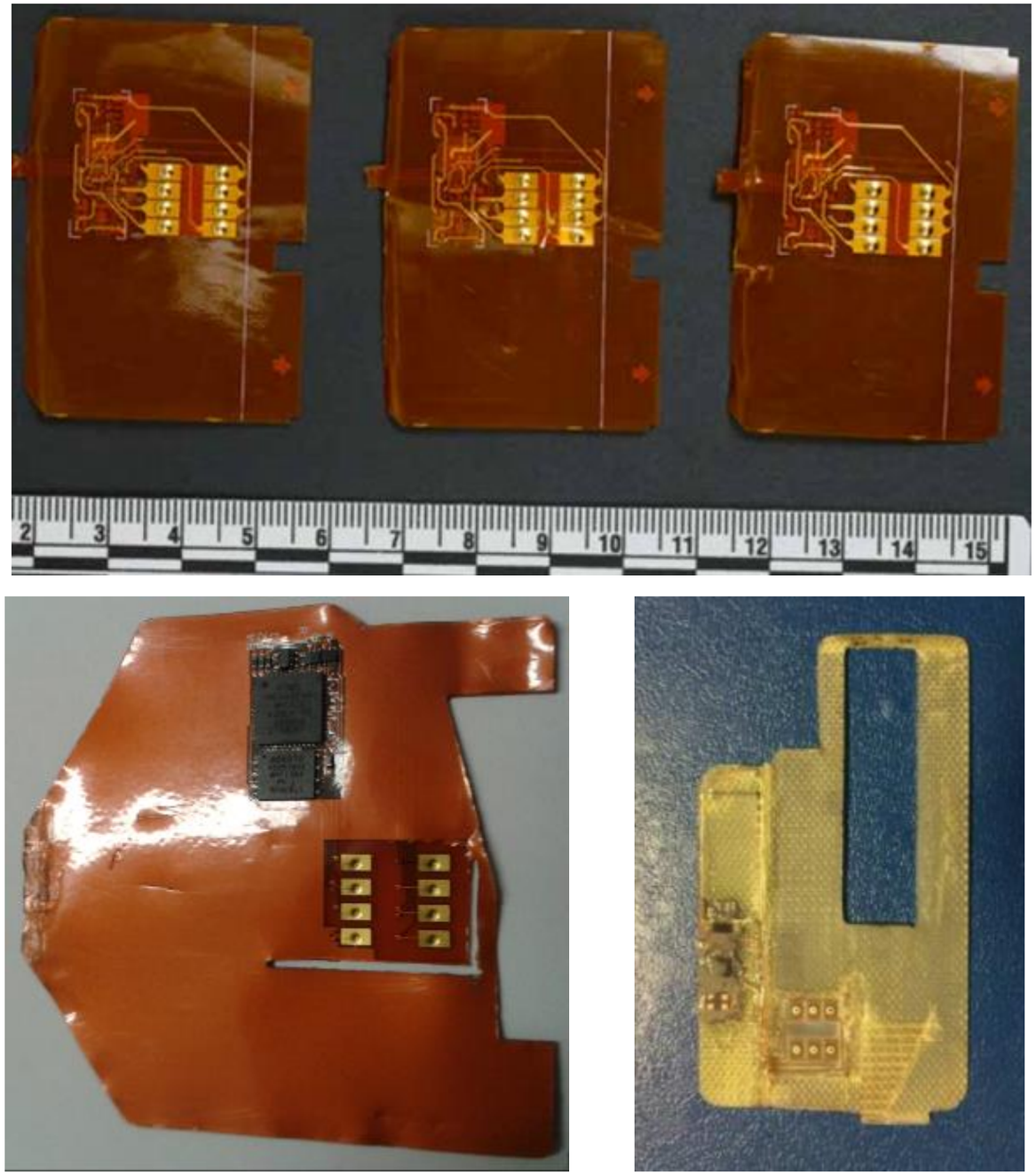
Infantry

U.S. M-4A1 and Chinese CQ 5.56mm Assault Carbine

EMV Card Cloning

Shimmer: portmanteau of

- **Shim**: a paper-thin, card-sized device with an embedded microchip and flash storage that copies and saves info from EMV card and
- **Skimmer**: a bulky device that lets a thief swipe a magnetic stripe credit card and record its info



Shimmers found in Canadian and Mexican point of sale devices and ATMs (Sources: RCMP, EAST, and Krebsonsecurity.com)

Methods of Chip Identification (ID)

- **Traceability** involves a unique chip ID to track each component as it moves throughout the supply chain
- **Detection** of Remarked, Overproduced, and Cloned provided the IDs are registered to a database
- **Requirements [1]**

  1) Unique, 2) Unclonable, 3) Manufacturable, 4) Reliable, 5) Cost Effective, 6) Easy-to-check

Within Chip

- Die ID, ECID
- PUF ID

In Package

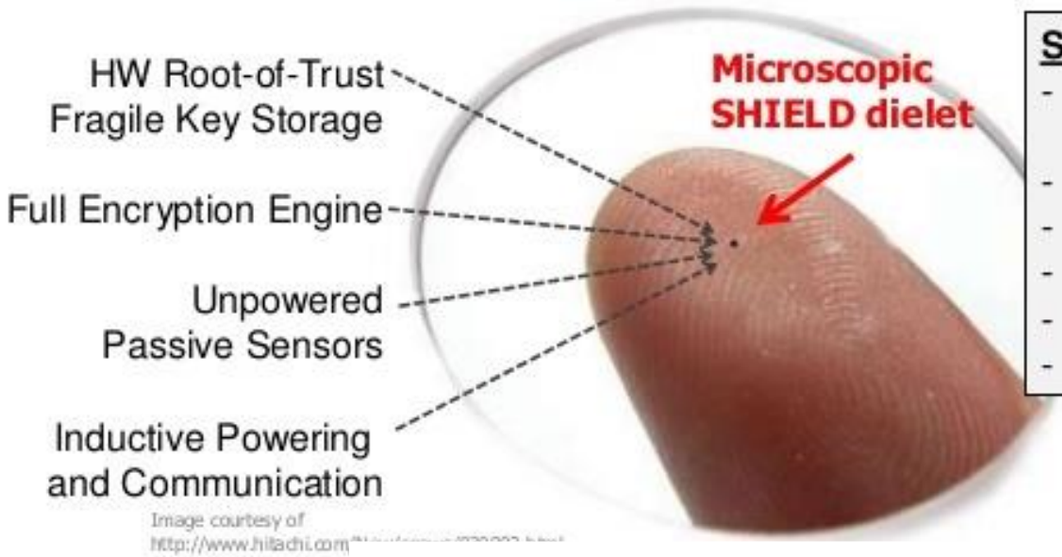
- SHIELD [2]

On Package

- DNA marking [3]
- Nanorods [4]
- QR Codes

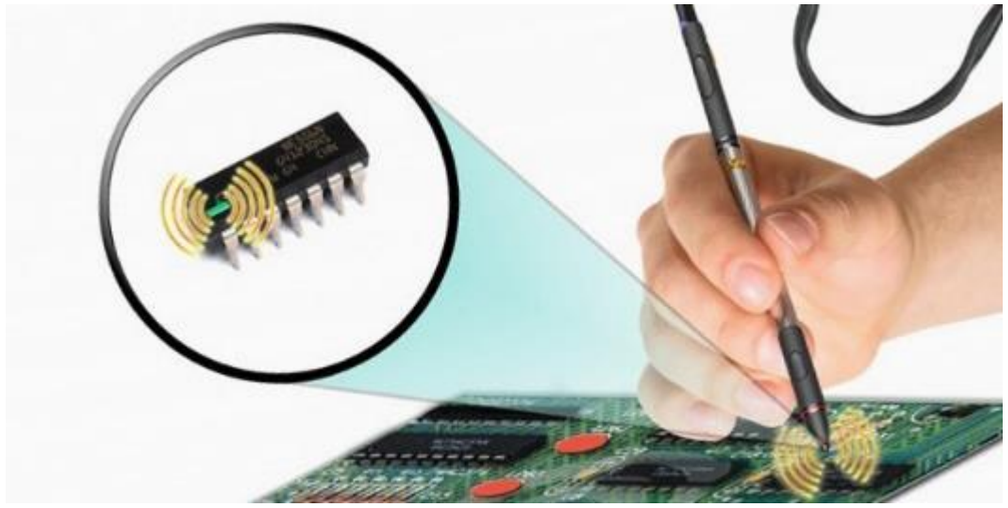
[1] Tehranipoor et al. Springer, 2015.
[2] DARPA, 2014
[3] Miller et al, SAE 2012.
[4] Kuemin et al, 2012.

DARPA SHIELD



SHIELD Target Spec

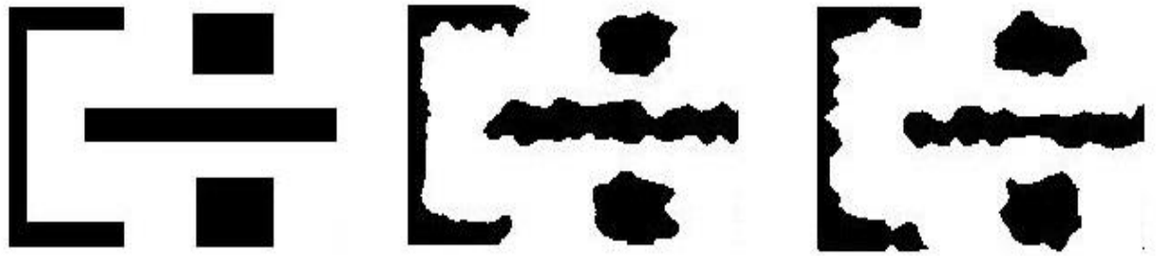
- 100µm x 100µm (0.01 mm² Area)
- 100K Devices
- 100 MHz Clock Rate
- 50 µW Total Power
- T ≤ 120°C
- <1¢ per dielet



Sources: DARPA, militaryaerospace.com

Physical(ly) Unclonable Functions

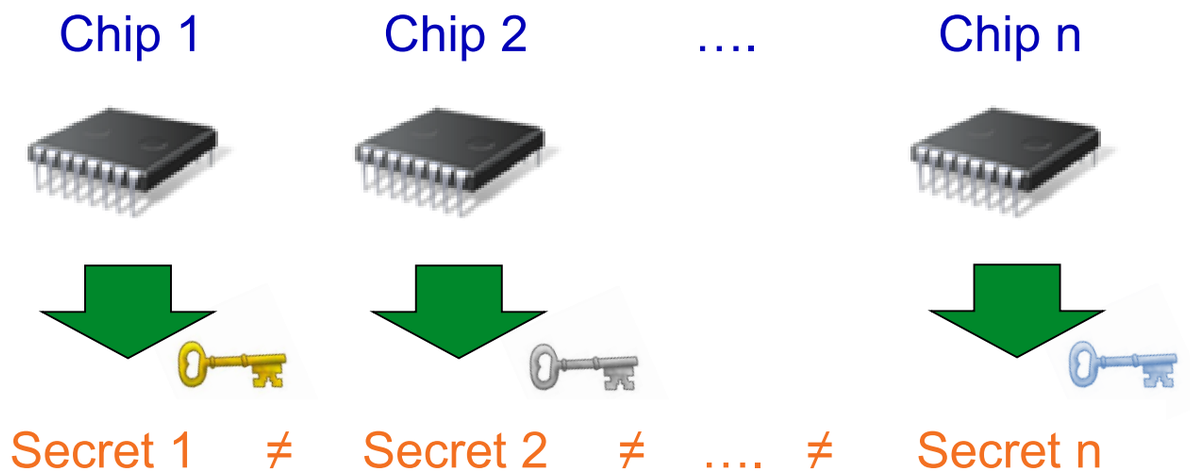
- Uncontrollable randomness present in physical structures of chip from manufacturing (~hardware biometric or fingerprint)
- A PUF is a circuit that extracts an internal, chip-specific secret based on the above randomness



Randomness in transistor length, width, gate oxide thickness, doping concentration density, etc.

Merits and Applications

- Better security and lower cost
- IC Identification/ Authentication, Safe Cryptographic Key Storage, and Tamper Detection

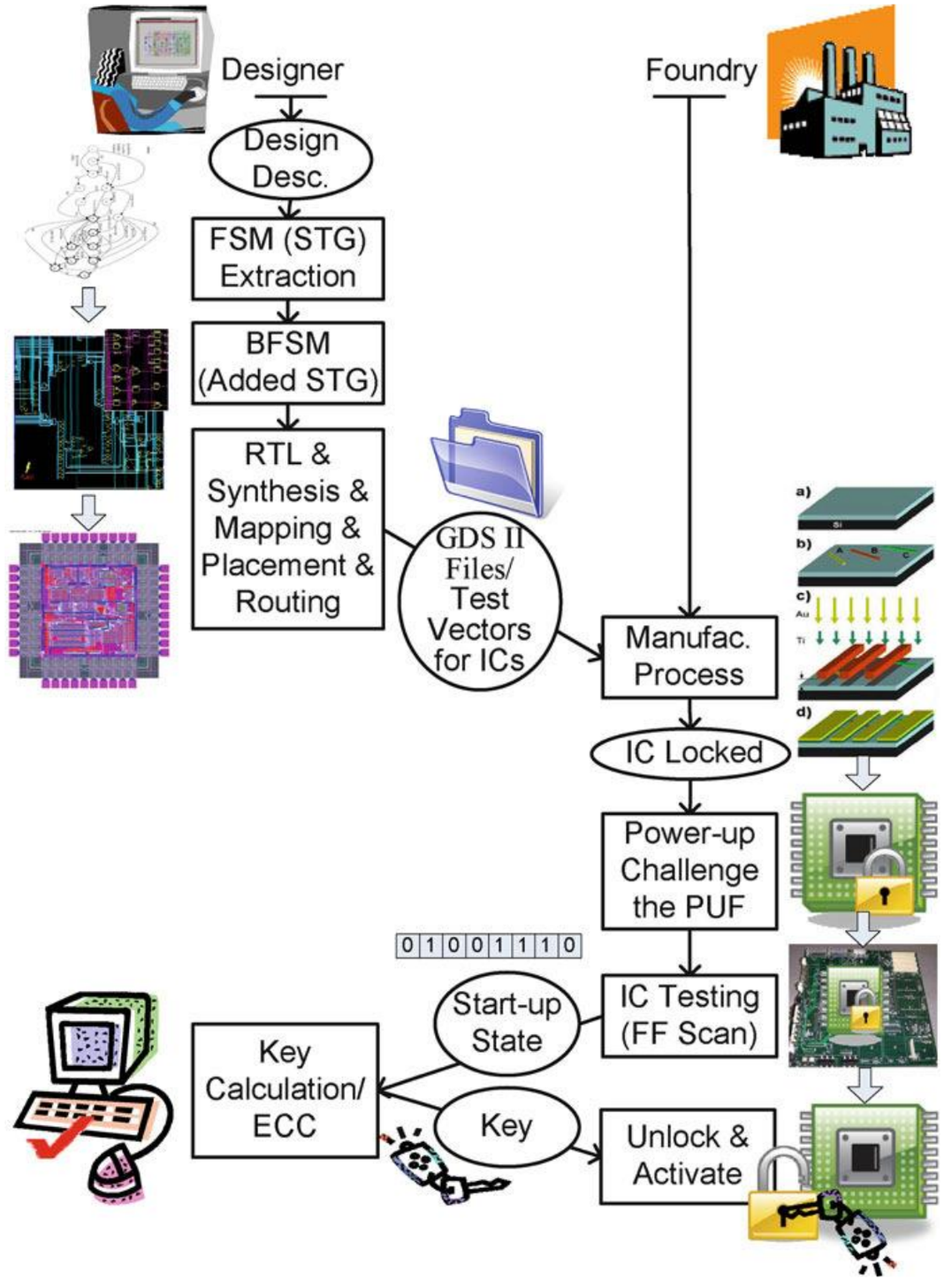


Hardware Metering (HM)

- The design house inserts locking mechanisms into the design
- The foundry receives the blueprint of the chip in the form of OASIS or GDSII files to fabricate the ICs
- After manufacturing, the foundry scans a PUF generated unique ID from each IC and sends it back to the design house
- The design house then sends an unlock key to the foundry to unlock the IC
- In theory, this allows design house to monitor number of activated chips **(prevents overproduction and cloning)**

Major Flaws:

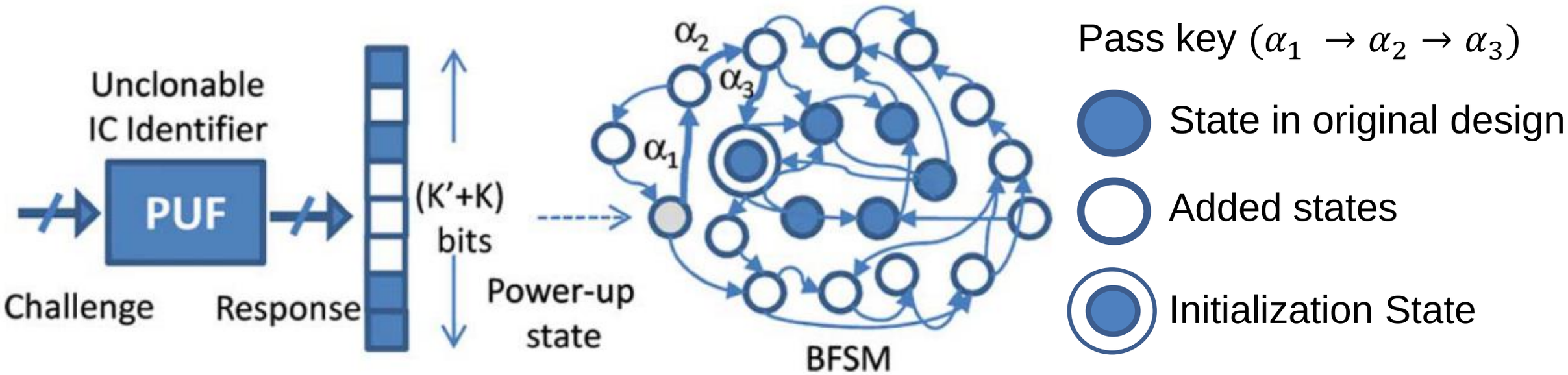
- Ignores the test flow and Assembly
- Foundry controls testing and can lie about yield to unlock additional chips



Source: Koushanfar, Springer 2012

Active IC Metering

Source: Koushanfar, Springer 2012



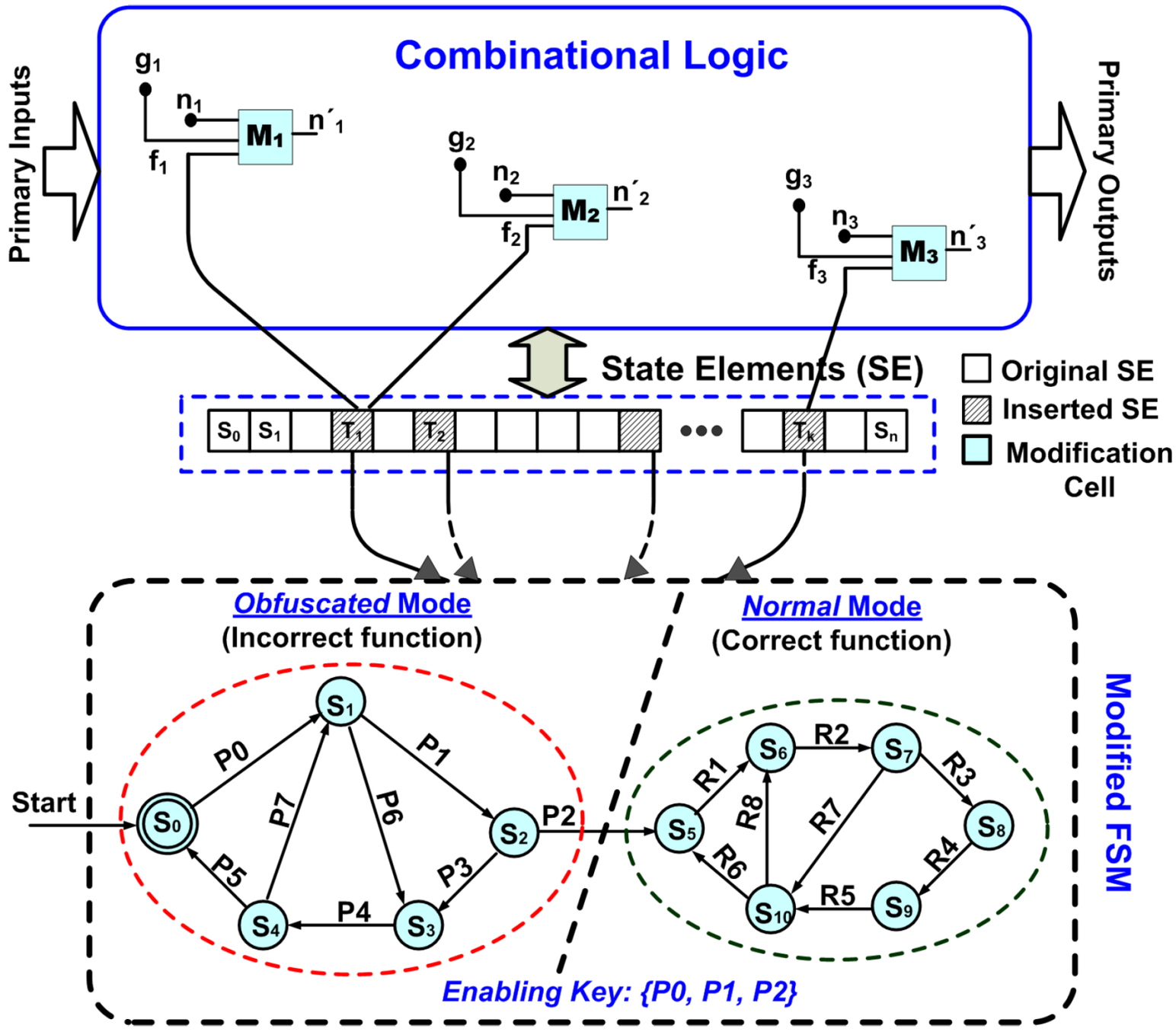
- BFSM composed of K (original) + K' (added) flip-flops
- Assuming $2^{K+K'} \gg 2^{K}$, the probability that the PUF response will initialize the design to an added state is very high
- Since the design house has the complete BFSM, it is ‘easy’ for them to compute a pass key to properly initialize the FSM

HARPOON

Obfuscated mode:
Incorrect functionality

Normal mode:
Correct functionality

- Start in “obfuscated mode” of FSM
- Key (enabling sequence) creates transition to “normal mode” of FSM



Source: Chakraborty et al., TCAD 2009

Secure Split Test (SST, CSST)

Designer

Secure Split Test

Design House must be included in test process

1. Functional unlocking key only known by the designer
2. Foundry/Assembly cannot distinguish between good and defective chips

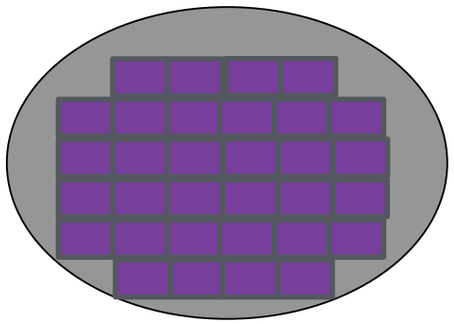
Design Additions

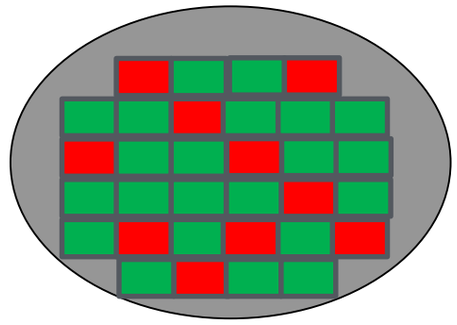
1. Designer adds hooks into the design that ensure non-functional operation if the correct key is not included in the chip
2. Designer includes TRNG for random perturbation in scan chain to ensure unique test responses per chip
3. Public/Private key crypto used to transfer data between Designer & Foundry/Assembly

Foundry & Assembly

Source: Contreras et al, DFT, 2013

CSST Flow





Signature (SIG_{FAB}) of Perturbed Resp. (PR)

$ECID$ and Encrypted TRNs

Foundry

Test all die and collect responses

Pass/Fail Check For Foundry

$ECID$s (Pass)

R_{IP} (avoids collusion)

Assembly

Package and test chips

Pass/Fail Check For Assembly

Signature (SIG_{ASMB}) of Perturbed Resp. (PR')

Generate FKEY for ECID (Pass)

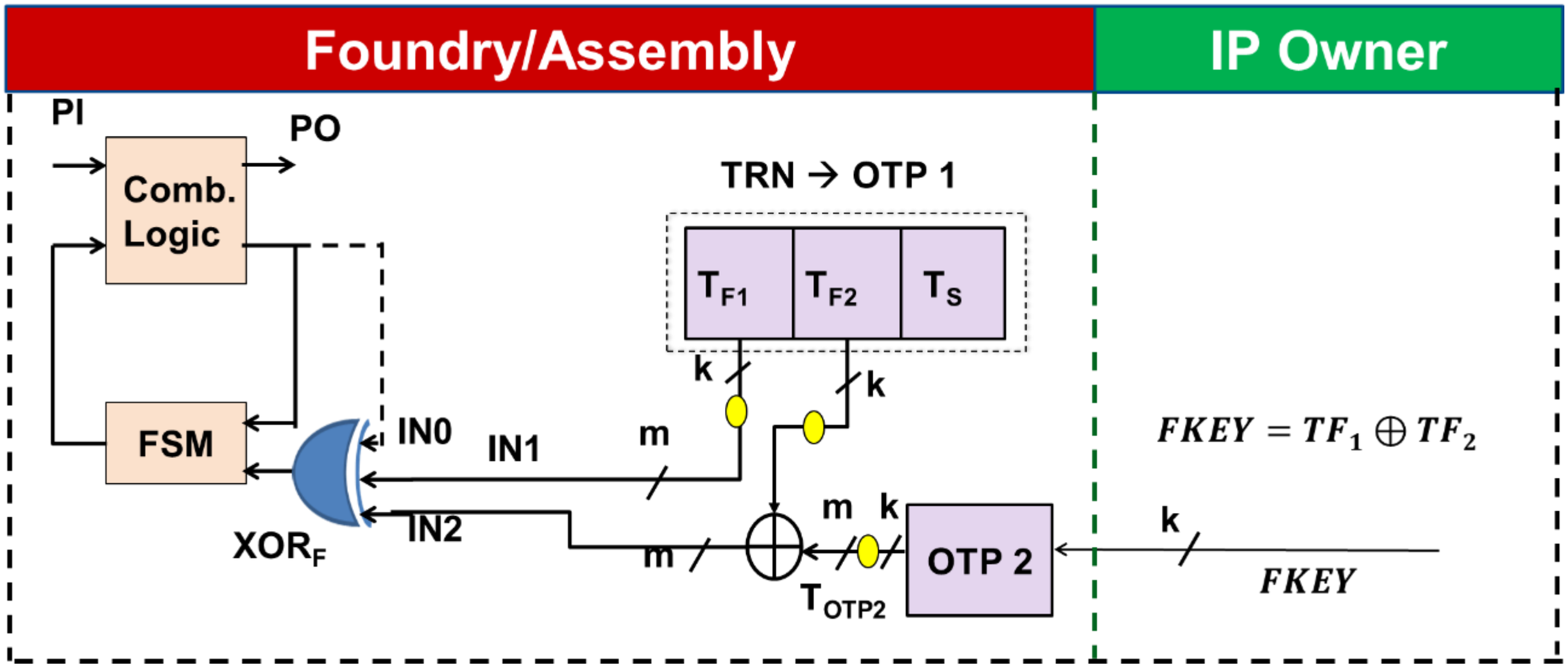
Unlock

Send $FKEY$
(unique to each chip)

IP Owner (Server)

Source: Rahman et al., DFT 2014

Functional Locking Steps

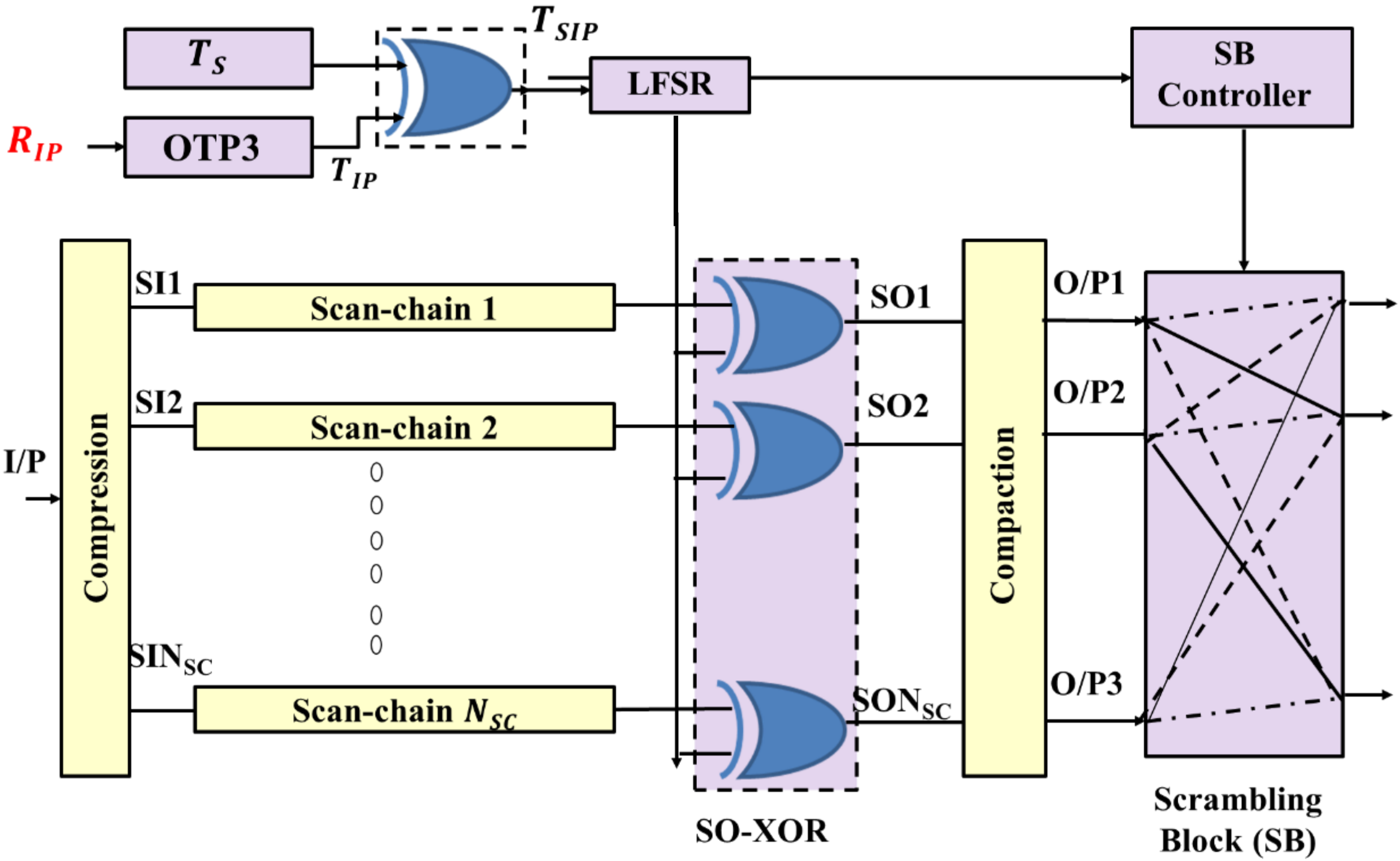


Notes:

- XORs are inserted on non-critical paths
- FKEY does not reveal TRN value

Source: Rahman et al., DFT 2014

Scan Locking Steps



Source: Rahman et al., DFT 2014

SST/CSST in Action

Design house only provides FKEYs for

1) Chips that pass tests at foundry *AND* assembly
2) Limited number of such chips

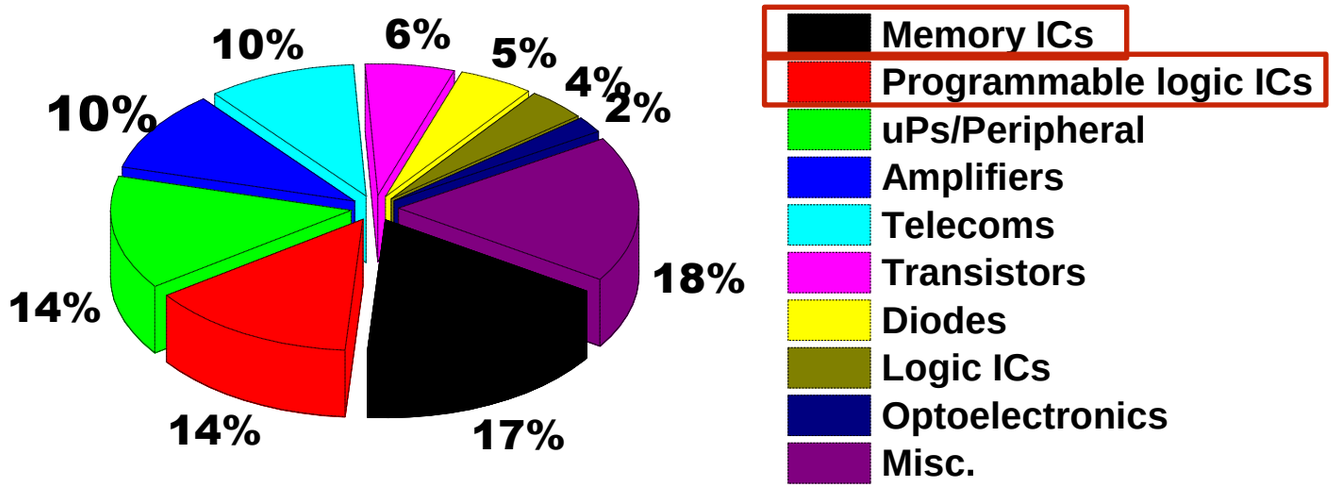
- #1 allows a consumer to easily identify out-of-spec/defective chips since they are still locked (produce incorrect output)
- #2 prevents overproduction and cloning in a manner similar to #1
- Further, design house can pinpoint the source of such attempts at counterfeiting

Note: SST may be vulnerable to invasive attacks, such as extraction of TRN or FKEY as well as design alteration.

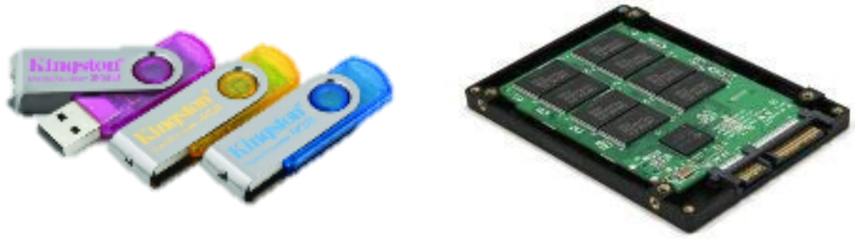
Section VI: Advanced Counterfeit Avoidance for FPGAs and Memories

Motivation

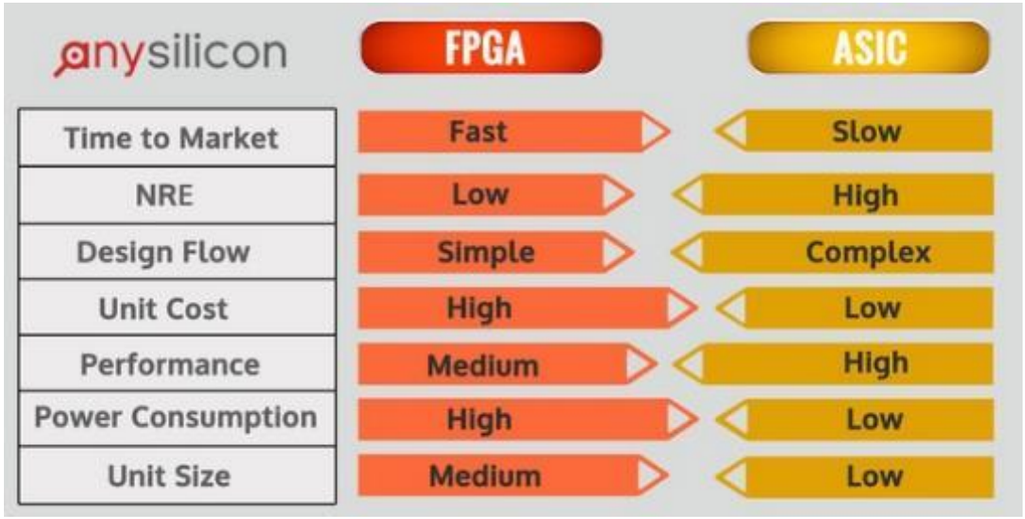
- Memories and FPGAs responsible for > 30% of counterfeits in the market
- Markets and applications (e.g., IoT) are growing for both cases
  - USB Flash and SSD drives
  - FPGAs have low non-recurring engineering (NRE) costs, low turnaround time, more capabilities, etc.
- Test setups for avoidance should be relatively easier than ASICs



Counterfeit report by device type (source: IHS 2016)



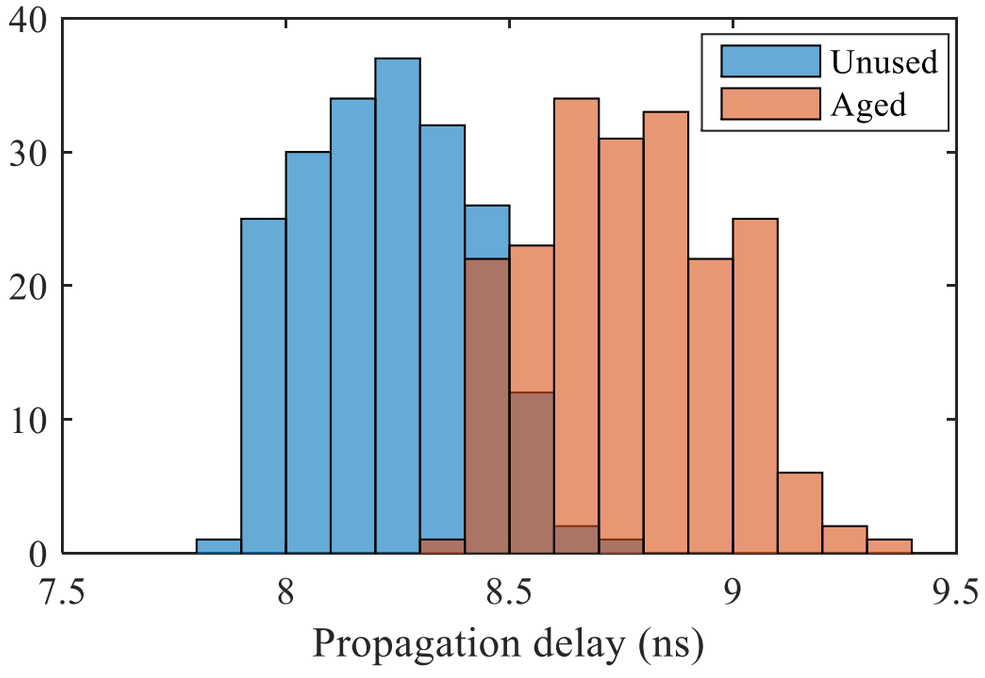
source: Google

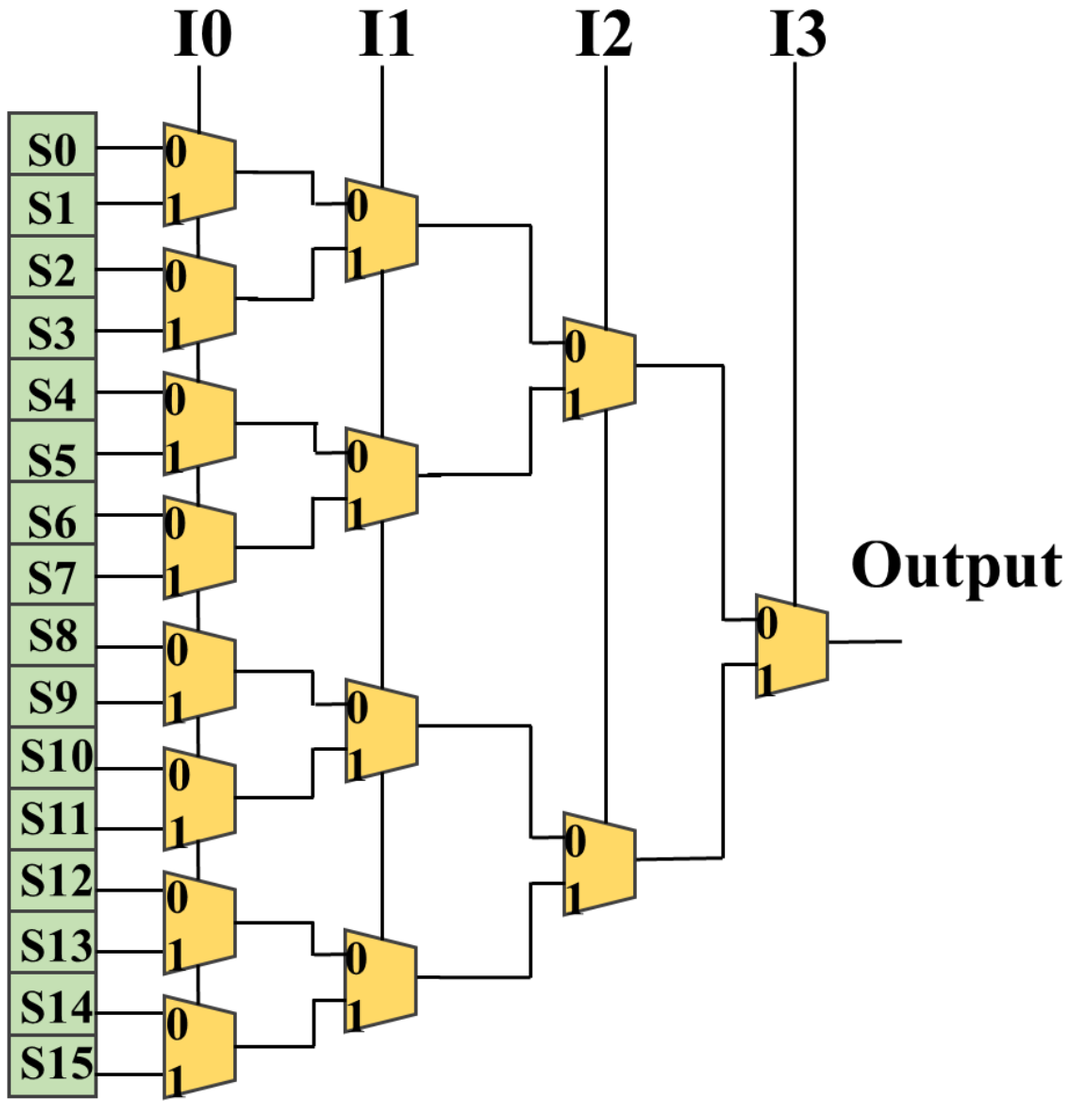


source: anysilicon.com

Impact of Aging on FPGAs

- Degradation in the threshold voltage of the MOS
- Degradation in the performance of interconnects
- Increased propagation delay of LUTs



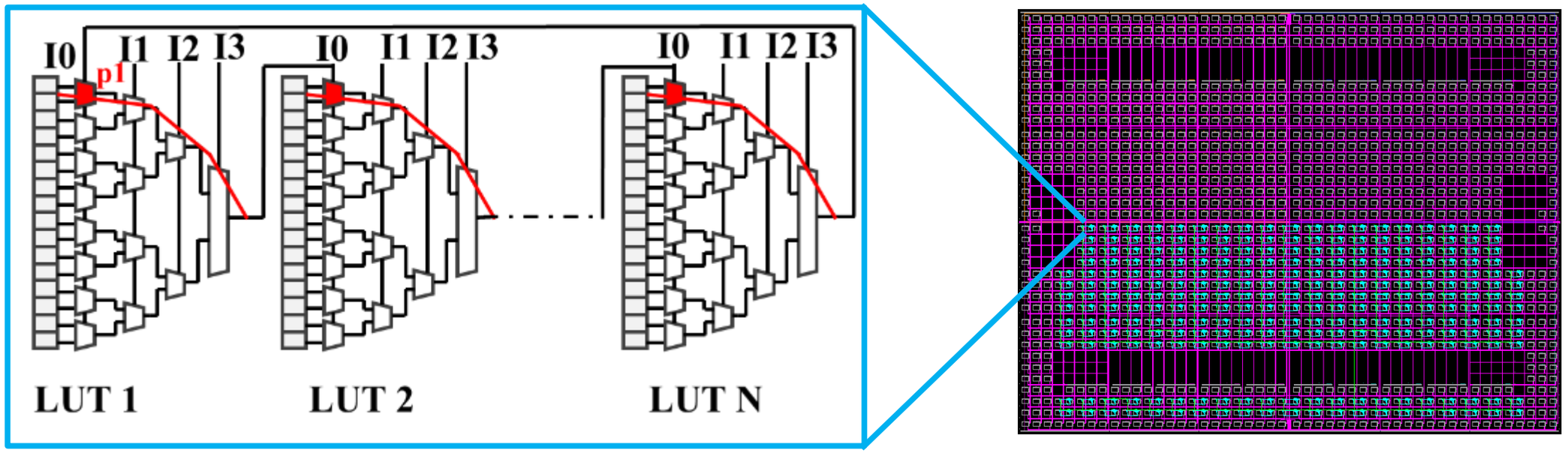


Look-up Table (LUT) Structure

Source: Alam et al., ITC 2016

Recycled FPGA Detection

No need for a built-in aging sensor! – program one in at any time, anywhere on FPGA fabric



RO Implementation in LUT

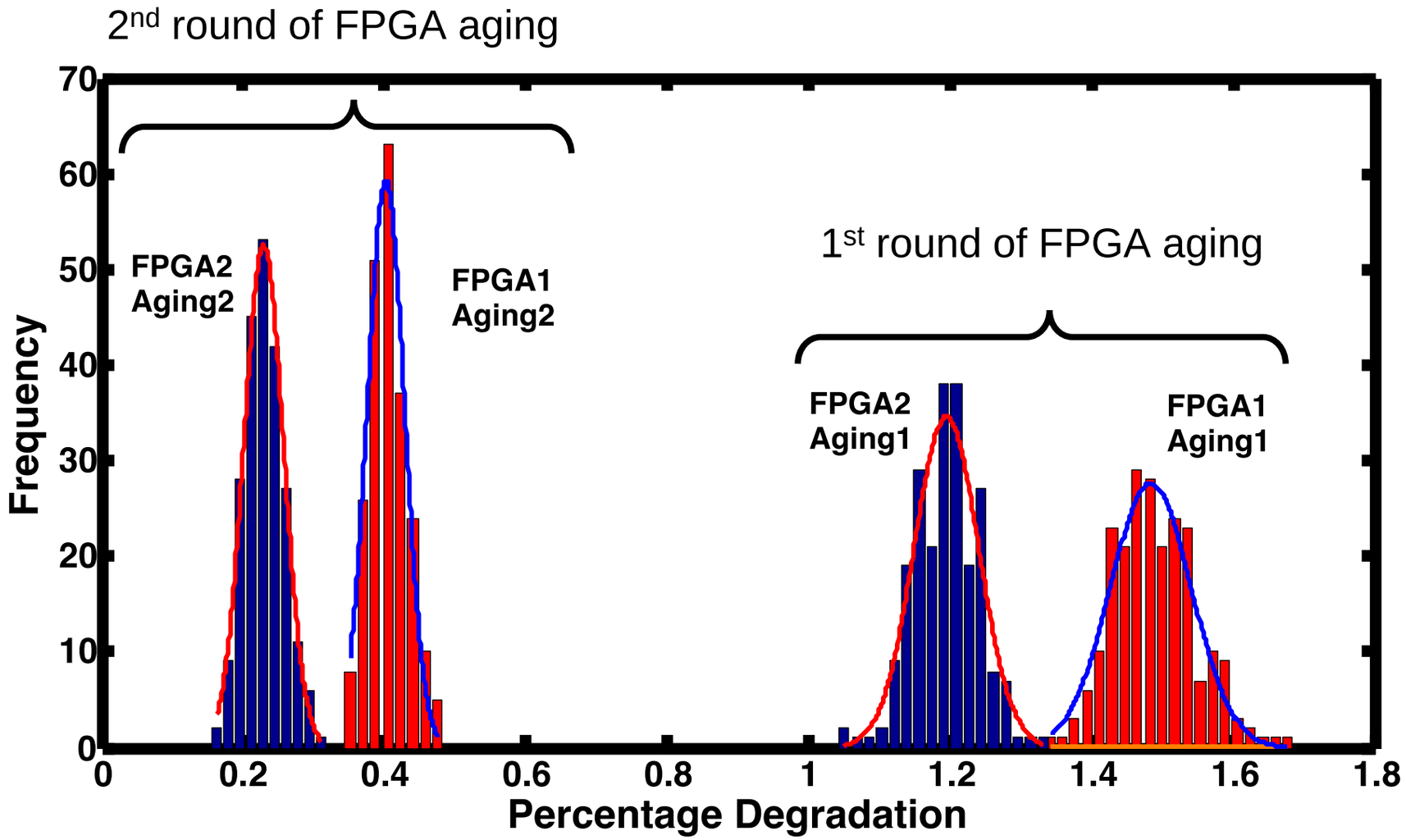
FPGA Layout

Source: Alam et al., ITC 2016

Exploited Characteristics

1) Rate of aging degradation (supervised, i.e., golden data known)
2) Variation in usage across FPGA (supervised and unsupervised)

Initial Approach (One LUT Path per RO)

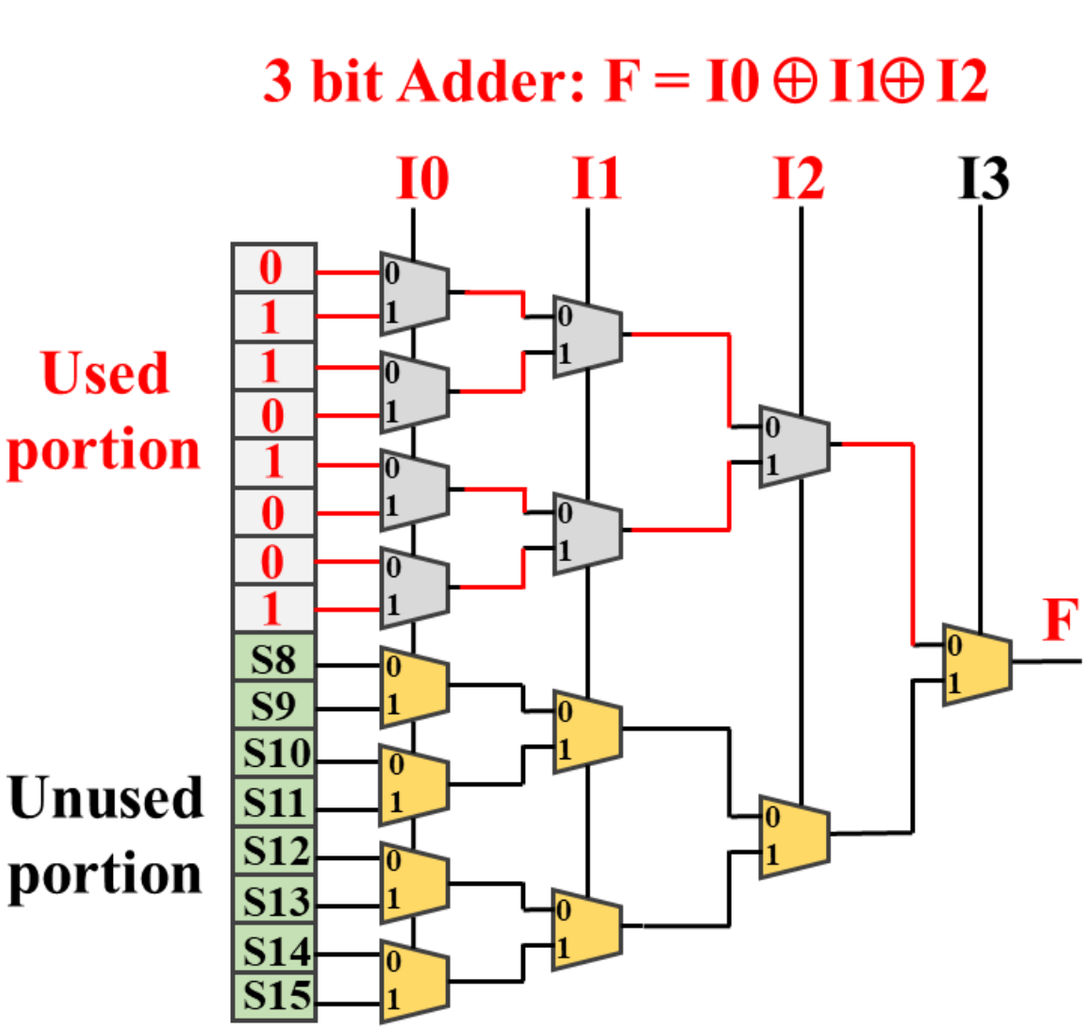


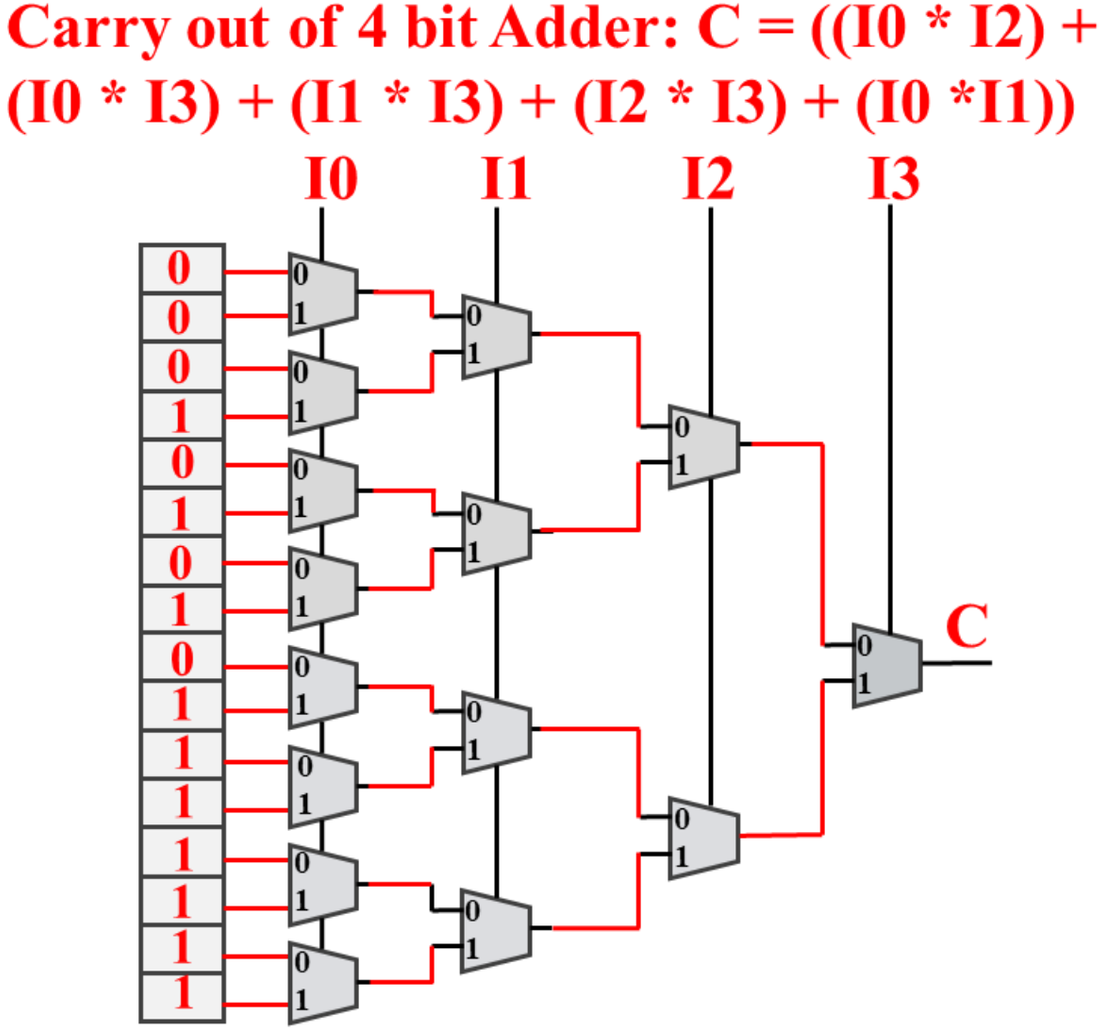
Source: Dogan et al., DFT 2014

Observation: Amount of degradation decreases with use

Disadvantage: Requires an accelerated aging step -> time consuming and partially destructive (performance degradation)

LUT ‘Types’ Based on Usage





(1) Partially Used LUT

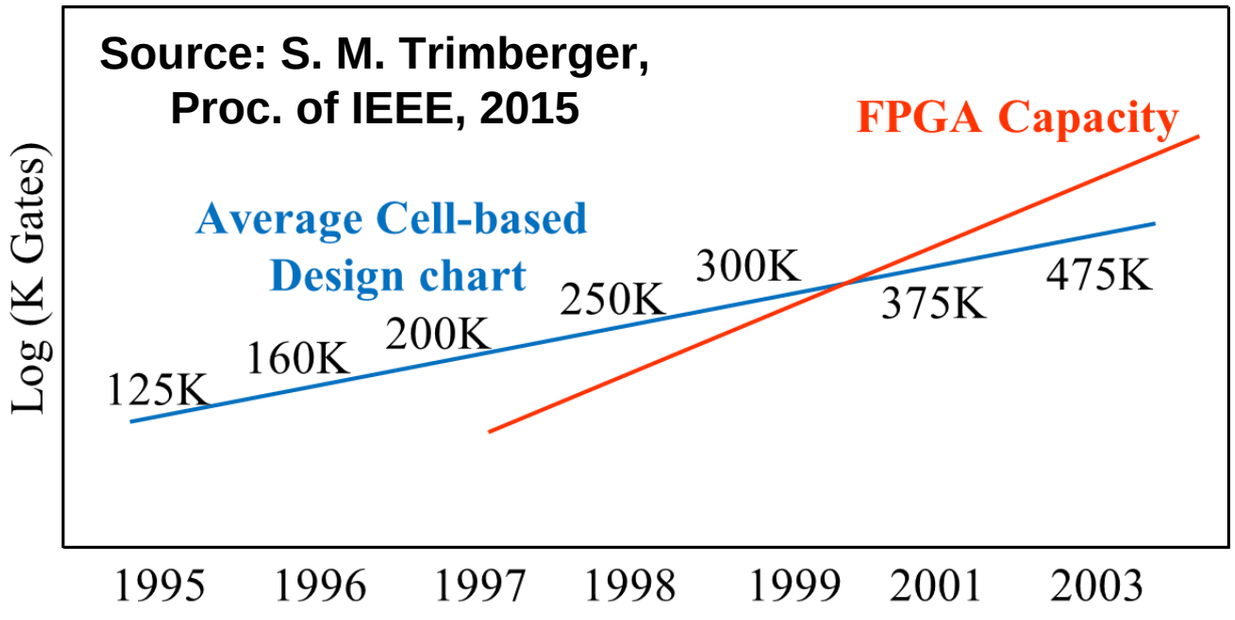
(2) Fully Used LUT

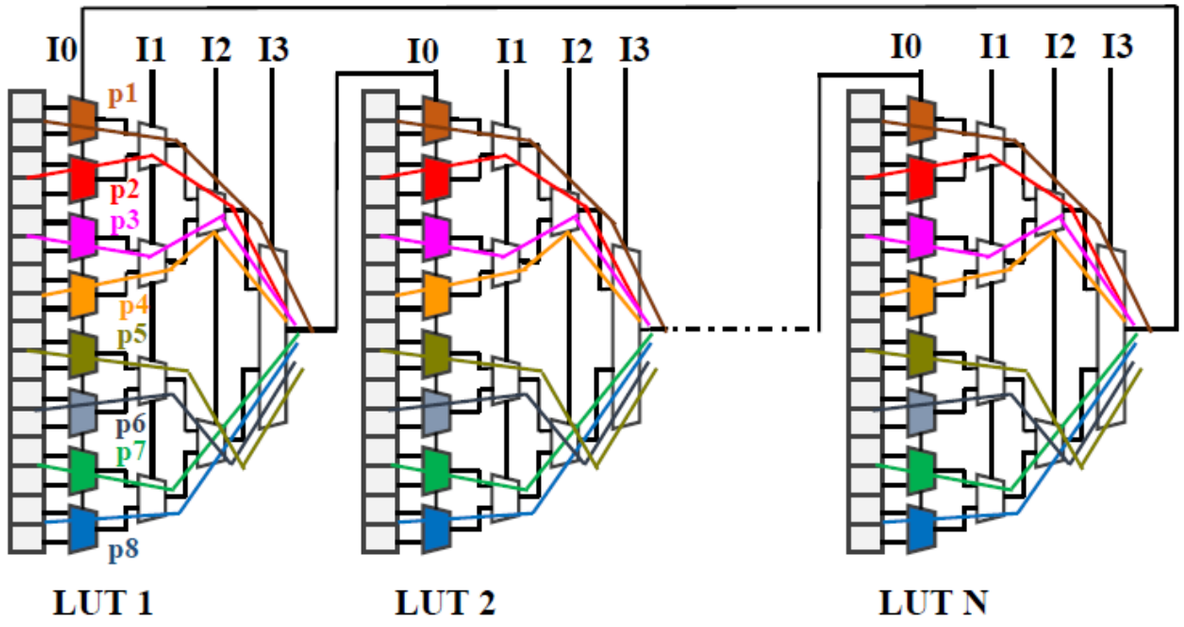
Source: Alam et al., ITC 2016

LUT ‘Types’ based on Usage Cont.

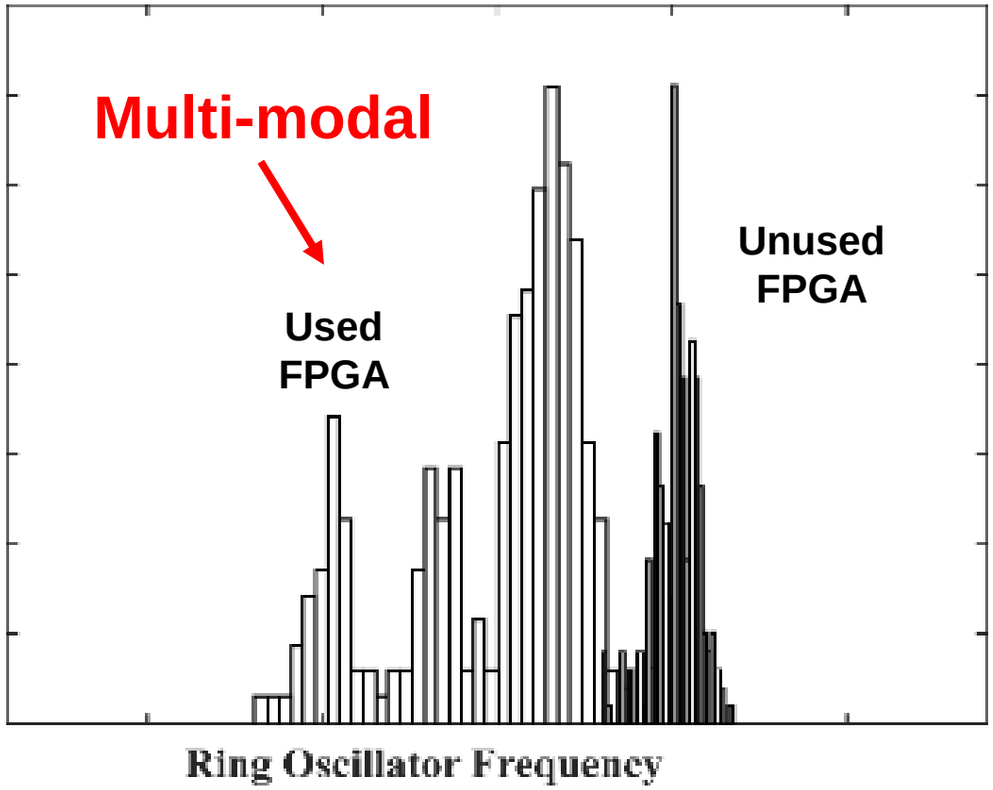
(3) Unused LUT

- All the available logic resources are rarely used
- Aging degradation of these spared LUTs are less than the used LUTs





Configurable LUT RO Implementation



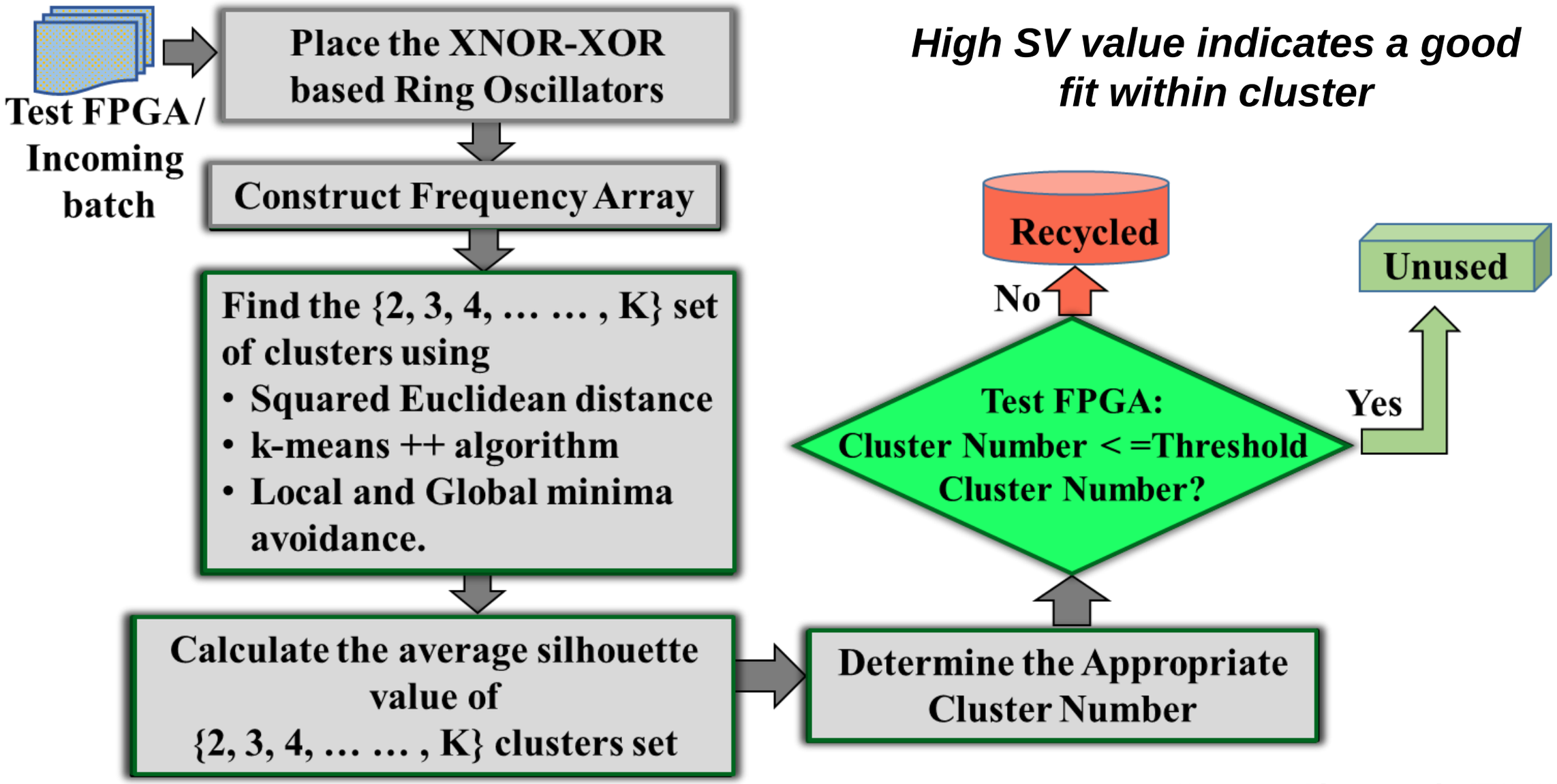
Source: Alam et al., ITC 2016

Unsupervised Classification

1) K-means Clustering partitions samples into k clusters by minimizing the average squared distance of cluster members to cluster means

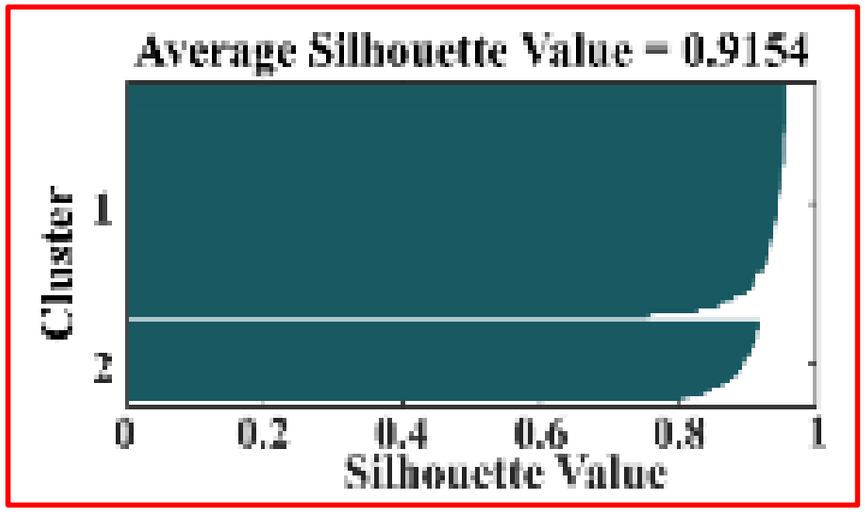
2) Silhouette Value (SV) tells how well a frequency fits within its own cluster and differs with the neighboring clusters.

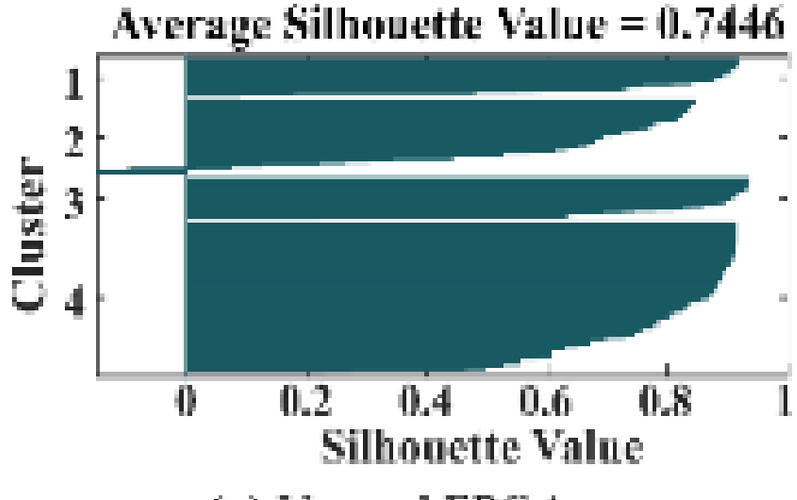
High SV value indicates a good fit within cluster

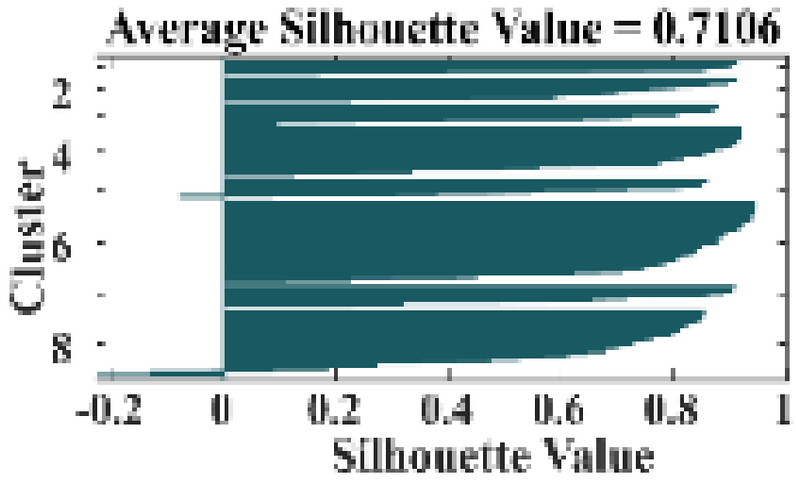


Source: Alam et al., ITC 2016

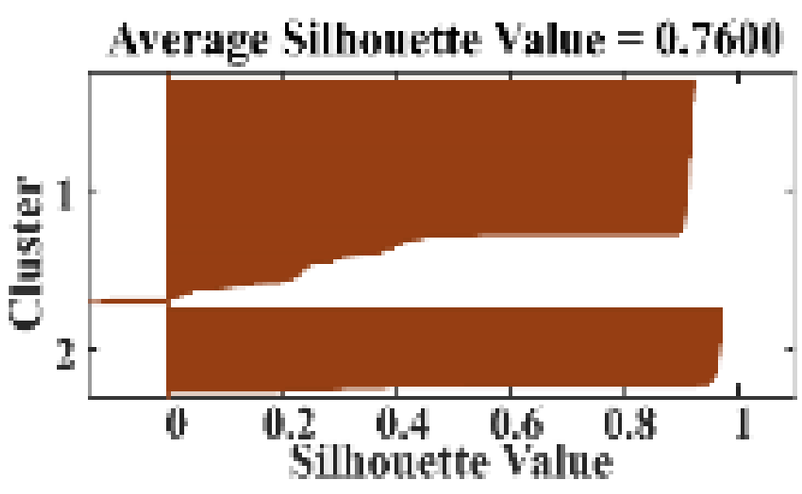
Silhouette Value (SV) Example

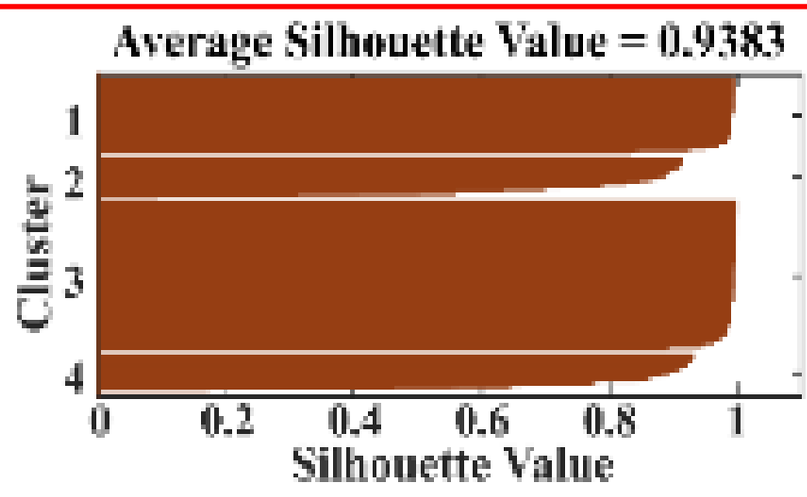


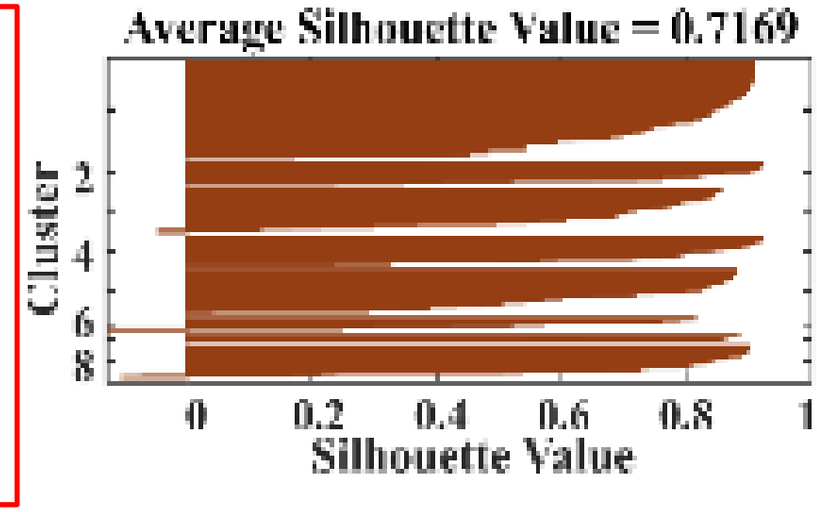




(a) Unused FPGA







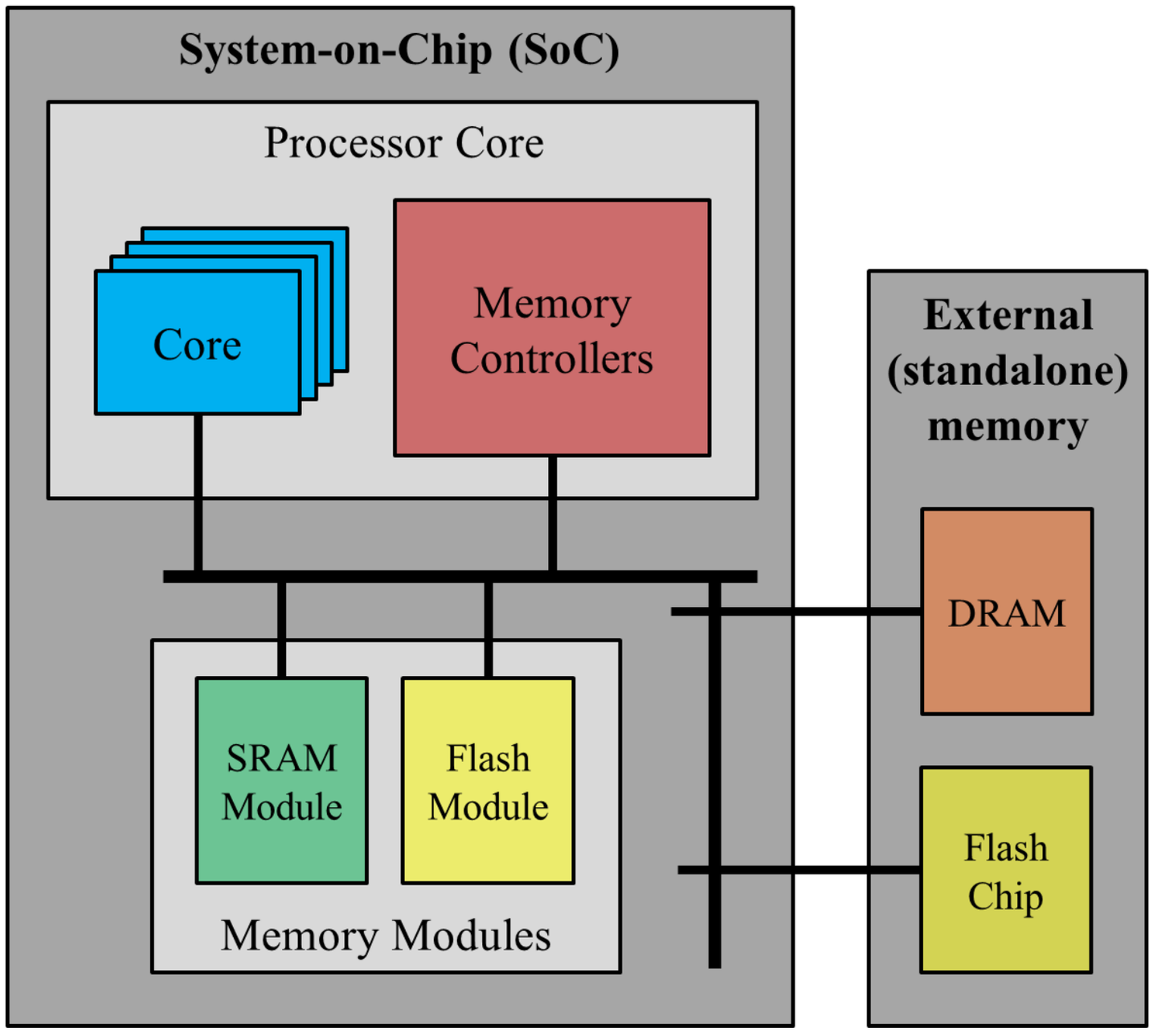
(b) Aged FPGA

Considering a threshold of 2 or 3 can distinguish between new and recycled FPGAs with high accuracy and without golden samples

Source: Alam et al., ITC 2016

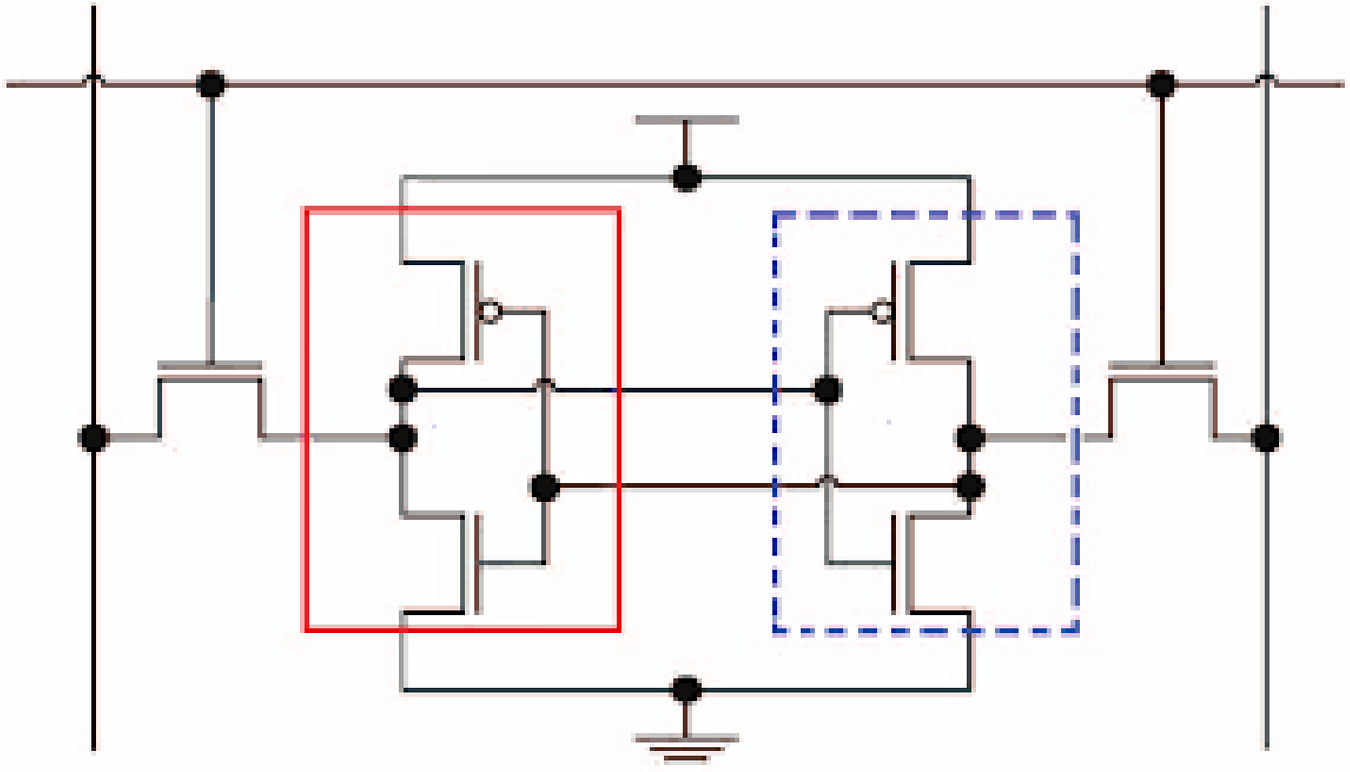
Memory-based Counterfeit Detection

1) Detect counterfeit memories without additional sensors
   - Anti-cloning (via memory-based PUFs)
   - Anti-recycling (via aging measurement)
2) Extends to system-on-chip (SoCs) with embedded SRAM (cache) and/or Flash

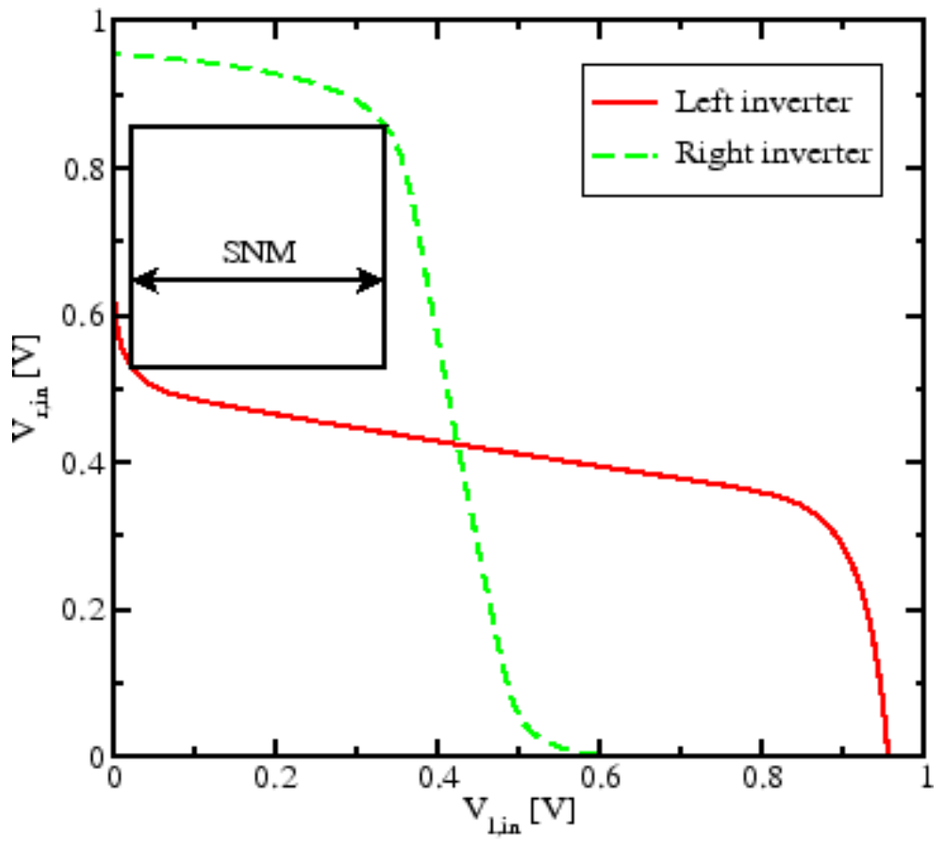


SRAM Start-up Behavior

Holcomb et al., IEEE RFID 2007
Guajardo et al., CHES 2007



6T CMOS SRAM Cell



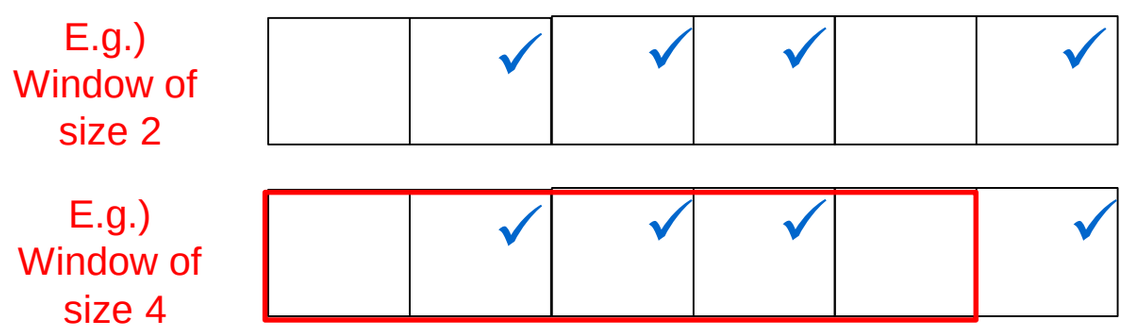
Static Noise Margin

- Cells favoring 0 or 1 at startup → ideal for PUF
- Cells that are random at startup → ideal for TRNG

Neighborhood-based Bit Selection

Xiao et al., HOST 2014
Rahman et al, HaSS 2017

✓ Denotes “stable” bit



Stable Memory Cells
(determined by enrollment)

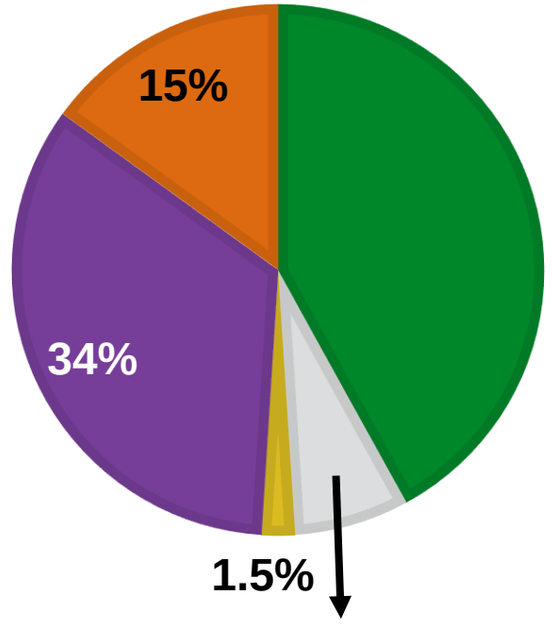
-	1	2	1	0	-
-	-	2	3	-	-

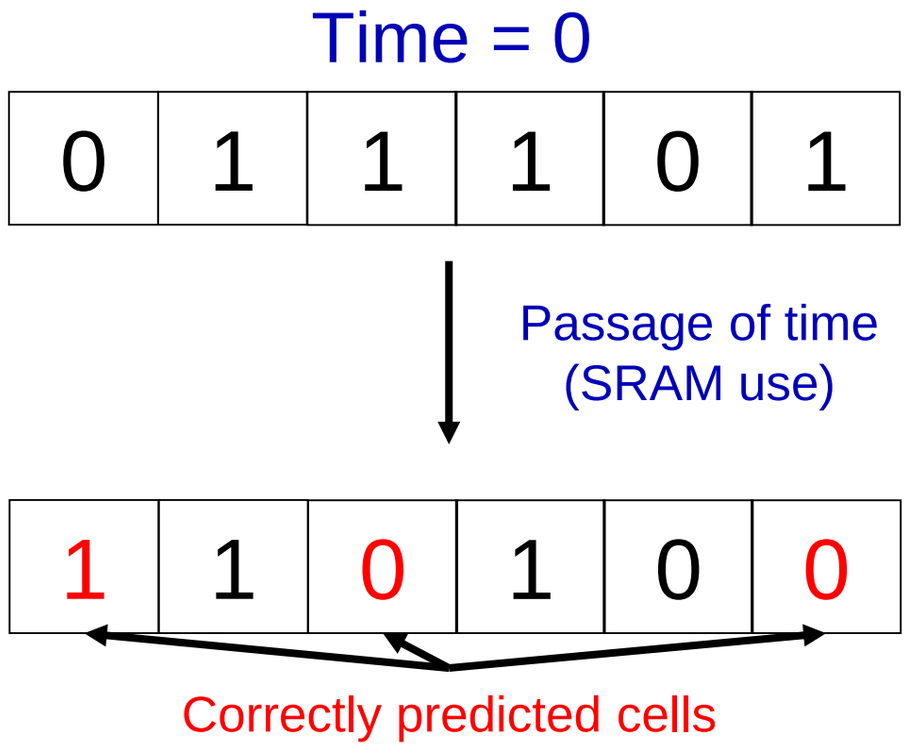
Out of four PUF candidates, one cell is chosen in this case

- Neighbor based Scoring Metric: Objective score of each cell is determined by taking a weighted sum of the stable bits surrounding it (estimated by enrollment)
- Threshold: For example, threshold is 3 (will scan the table for ≥ 3)
- Improvements (about three orders of magnitude) in bit error rate over time and extreme environmental conditions

SRAM-based Anti-Counterfeit

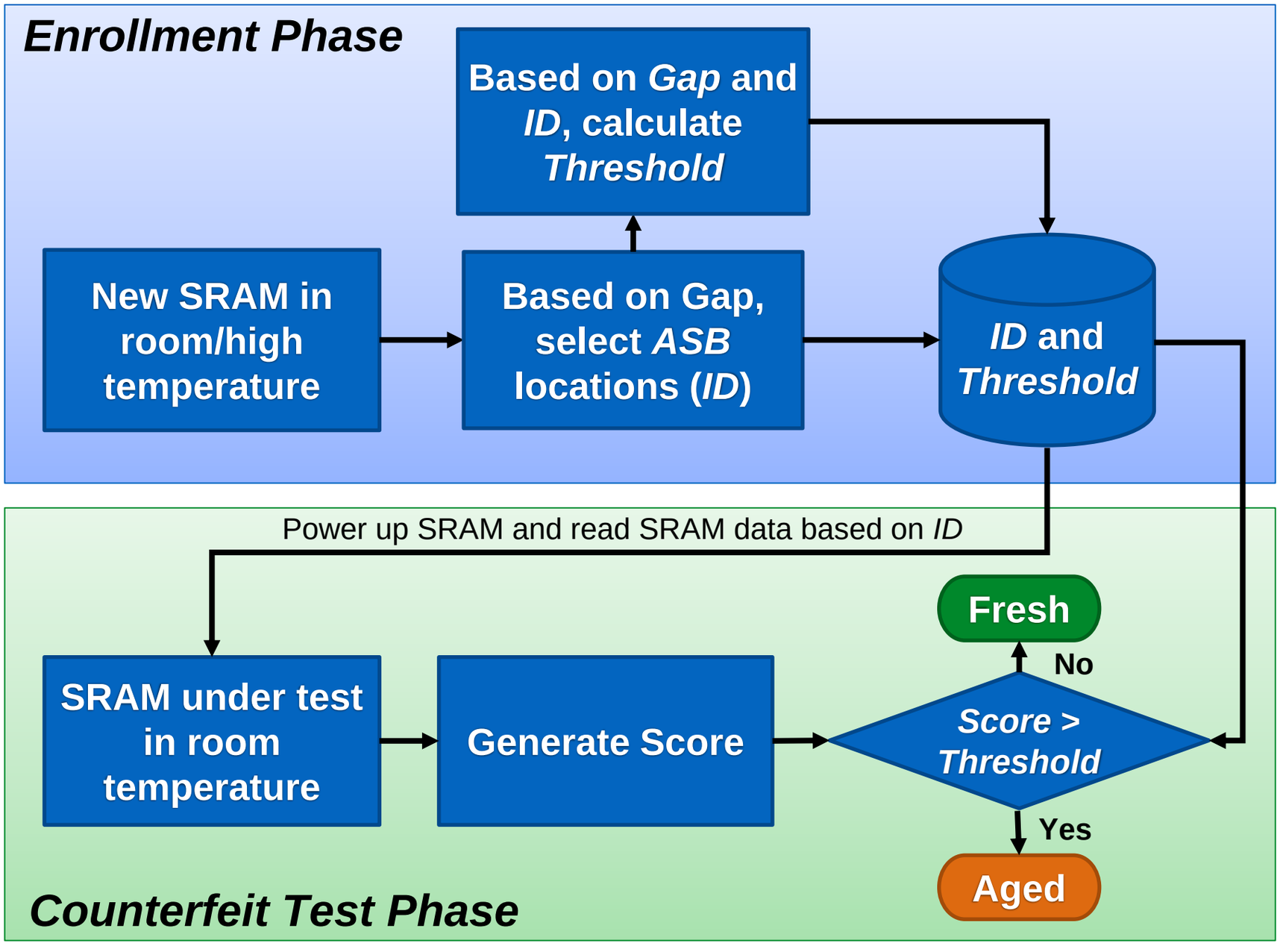
- Existing approaches for ASIC exploit aging and use method of self-referencing
- Extension to memory
  - **Basic Idea:** Initial stable ’0’s, stable ‘1’s change over time due to memory aging/usage
  - **Initialization step:** Aging sensitivity-based (ASB) bit selection





SRAM-based Anti-Counterfeit

Source: Guo et al., HOST 2016



ASBs: **A**geing-**S**ensitive SRAM **B**its
ID: ASB locations.

Important parameters
Gap: Designer-defined parameter.
Threshold: a value used to determined recycled IC ***(stored in some non-volatile memory)***

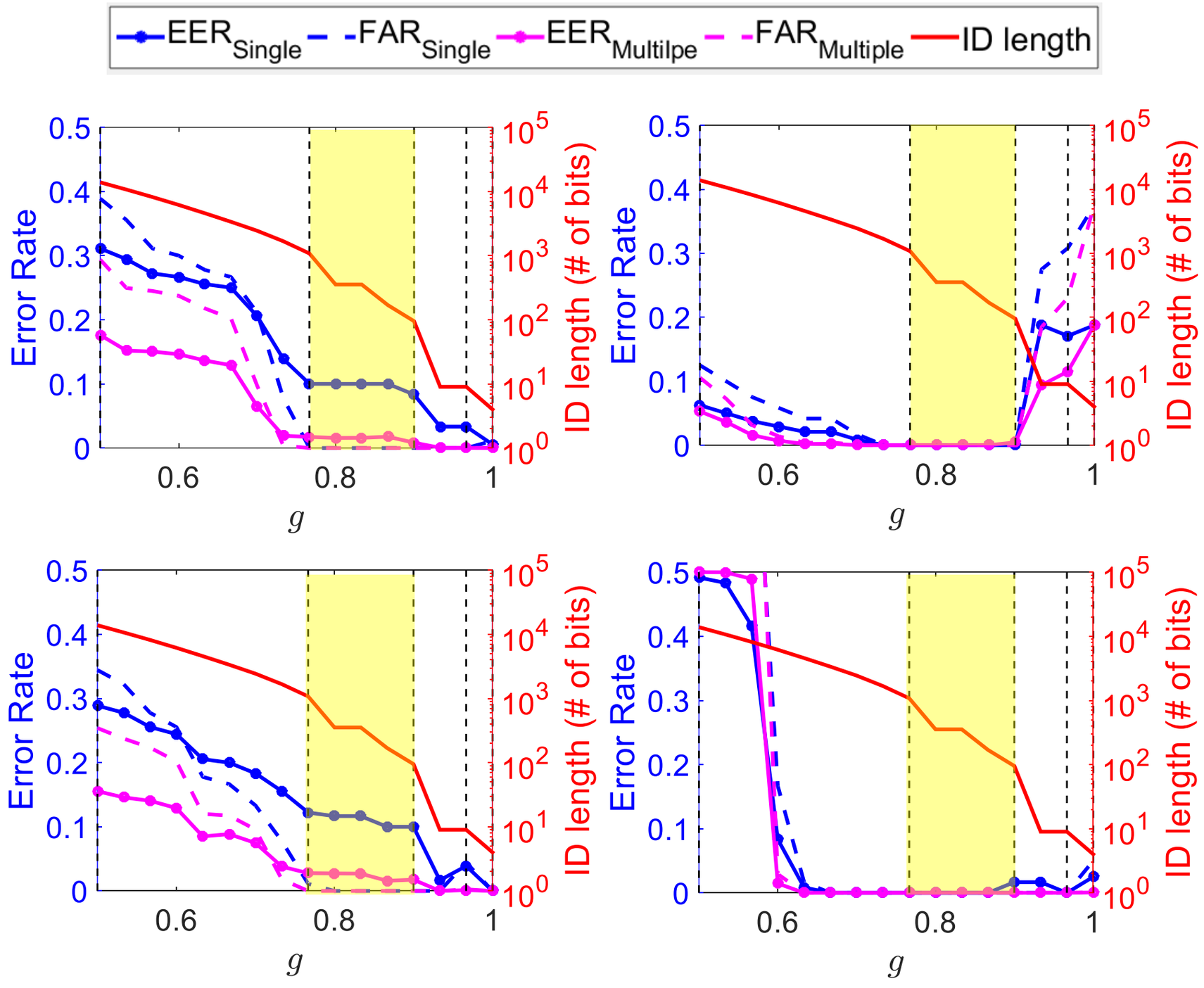
Counterfeit test
Score: a value generated by SRAM under test.

Classification Performance

Area 2: Good performance with respect to accuracy

SRAM #	EER	FAR
1	0.01	0.00
2	0.00	0.00
3	0.03	0.00
4	0.00	0.00

Further improvements in Guo et al., TVLSI 2018



Source: Guo et al., HOST 2016

Flash Memory-based Anti-Counterfeit

Why?

Critical Apps
(e.g. fighter jet, missile system)

1,500 flash memory chips bought by Raytheon were **counterfeit**

Non-critical applications
(e.g. Flash drive, SSD)

Reported by **Ebay**, **Kingston,** and **Toshiba** are particularly popular targets for **counterfeiting**

3-fold detection goals

Recycled flash determination	• **Yes-or-no** decision
Rough usage estimation	• Generate **rough usage assessment**
Accurate usage estimation	• **Refine** the assessment

Device signature (ID)

ID generation	• Generate **reliable**/ **unique** device ID

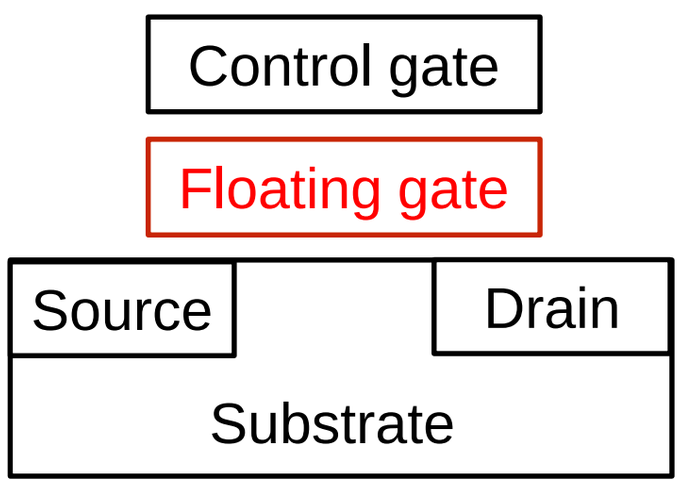
Advantages of exploiting Flash:

- ❖ *Non-volatility*
- ❖ *High density*

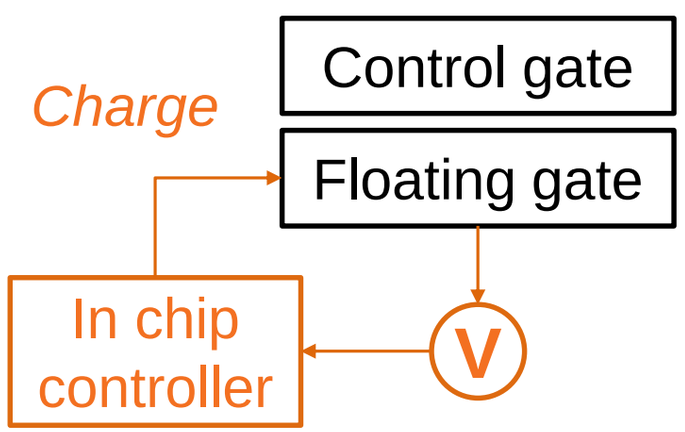
Flash Memory Background

- **Basic unit:** Floating Gate (FG) Transistors
- **Operations:** Program (Write), Erase, Read

Wang et al., IEEE S&P 2012

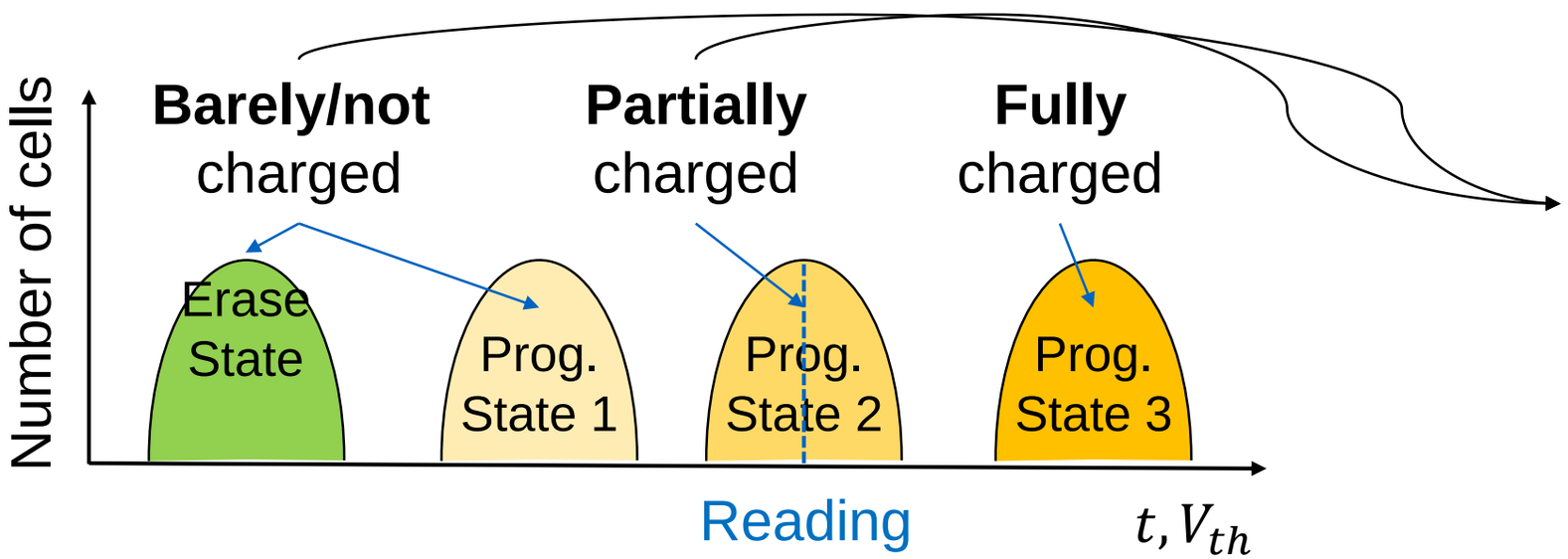


Floating Gate Transistors



Partial programing

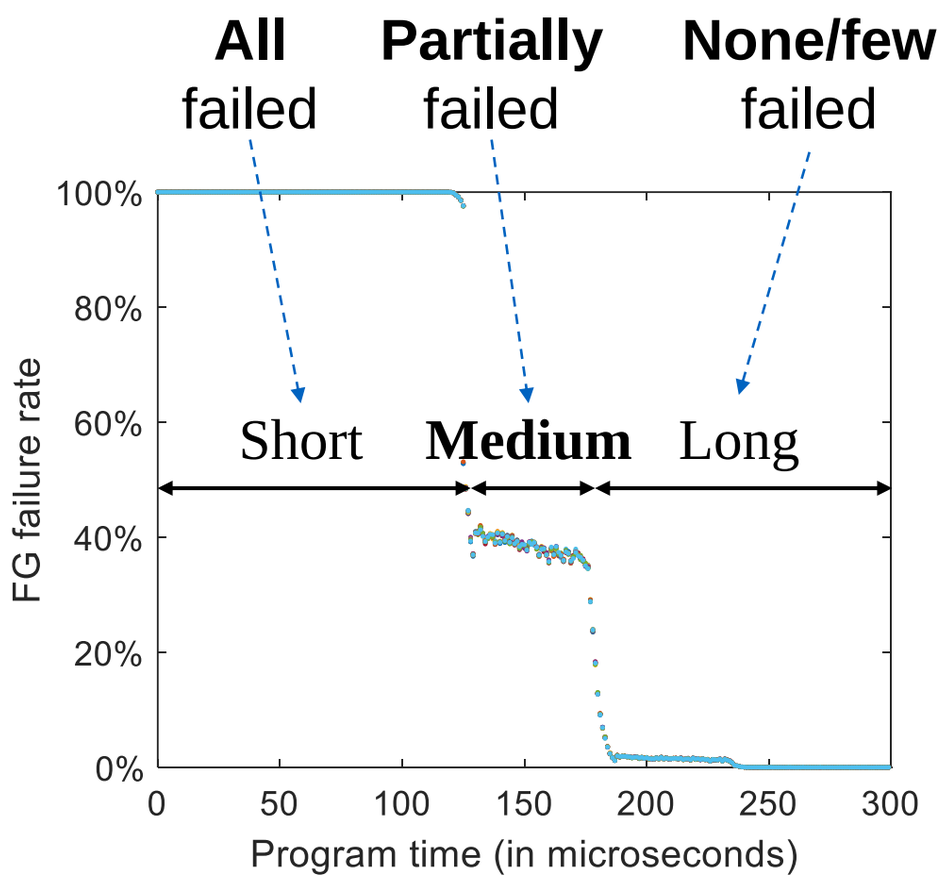
- Programming scheduling
- Process variations
- **Aging effects**

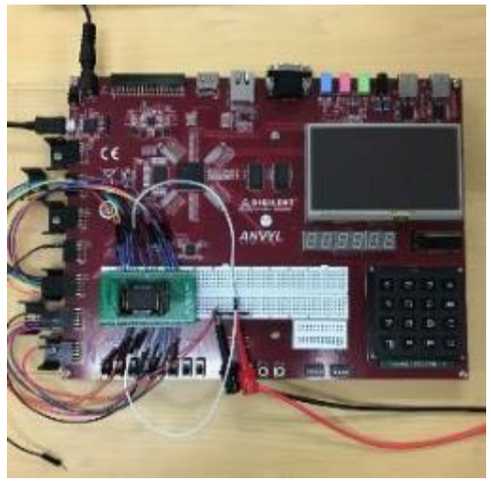


Induce FG failures

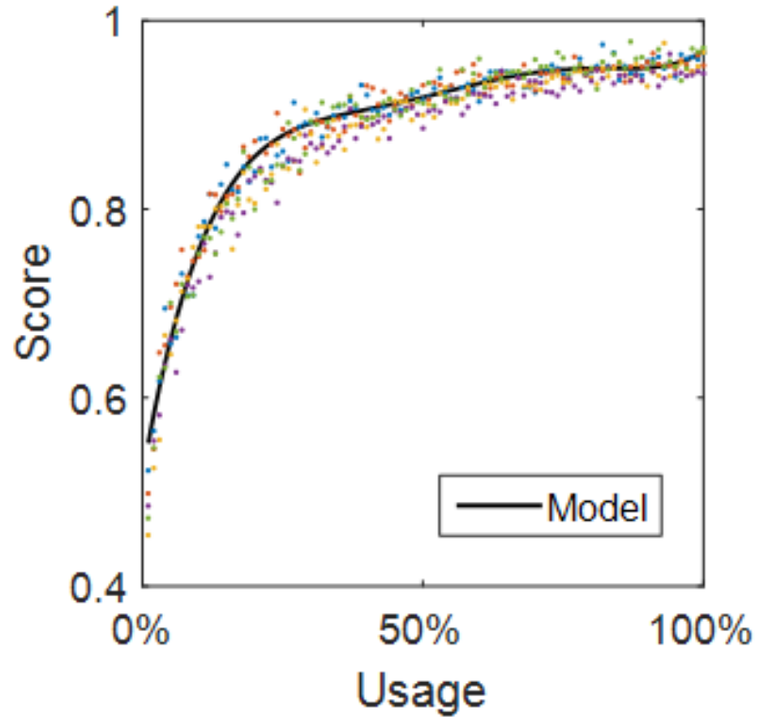
- Failure locations
- Insensitive to noise

Partial Programming vs. Aging



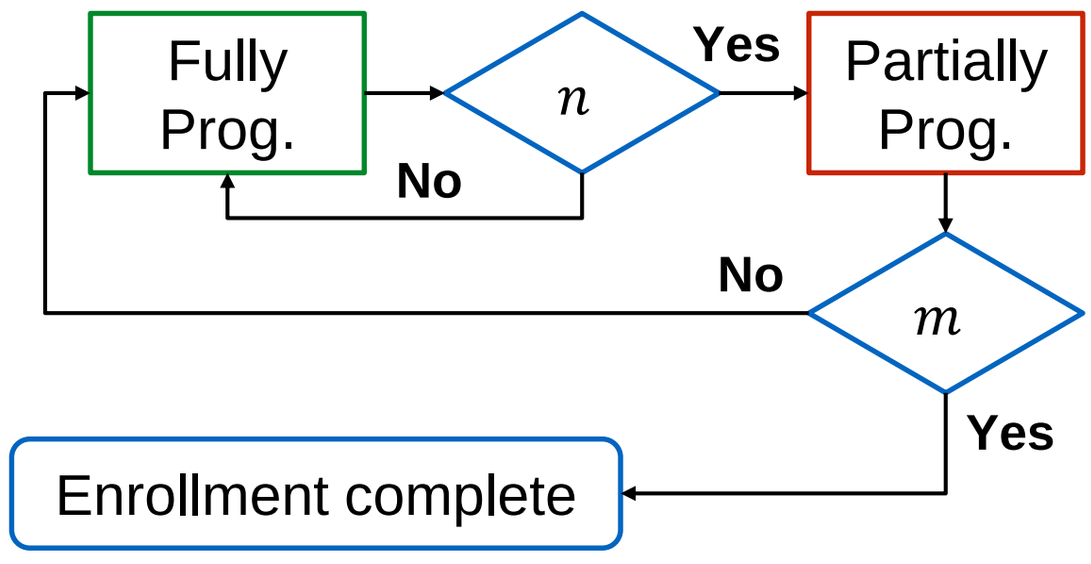


Source: Guo et al., DAC 2017

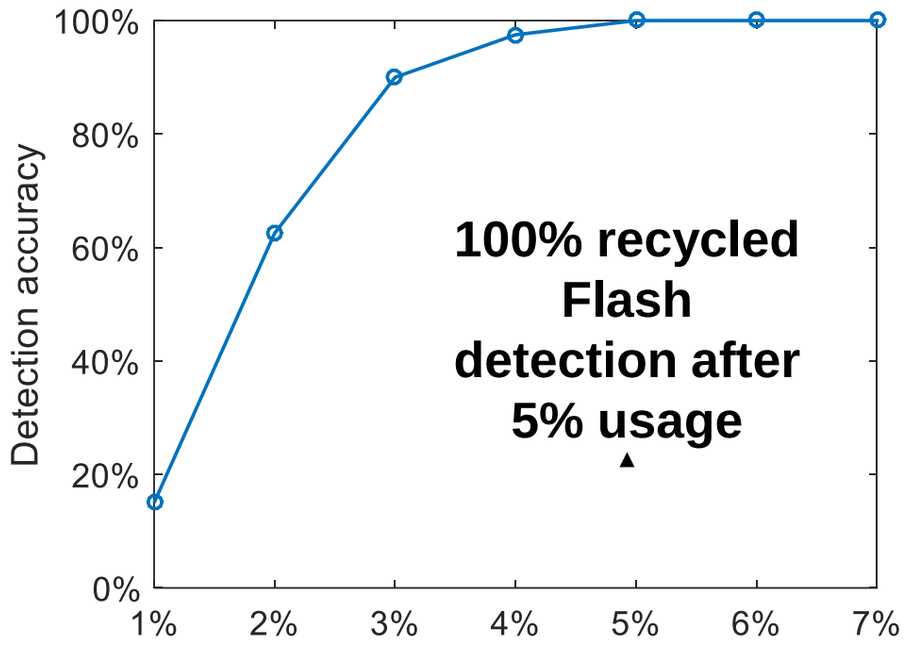


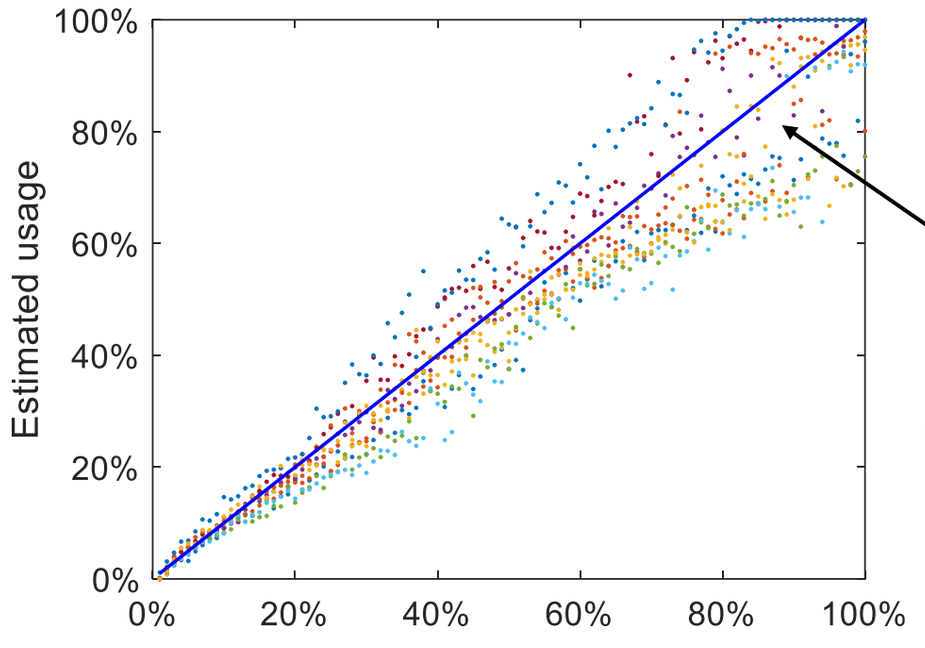
Endurance depletion (aging) and measurement: 1 partial programming is performed after every n full programs

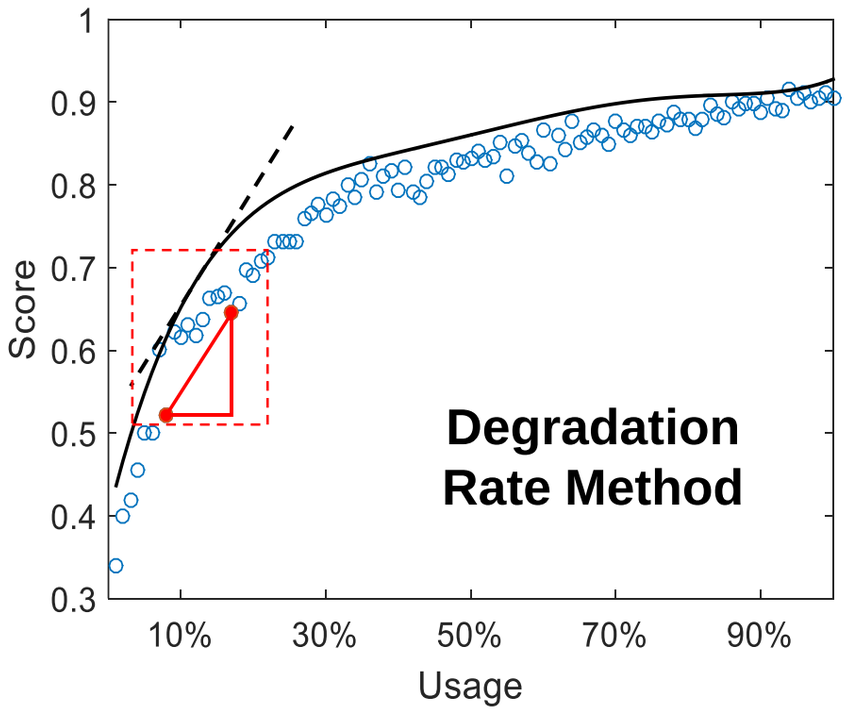
$$s_{i,j}(k) = f_i(u_{i,j}(k))$$

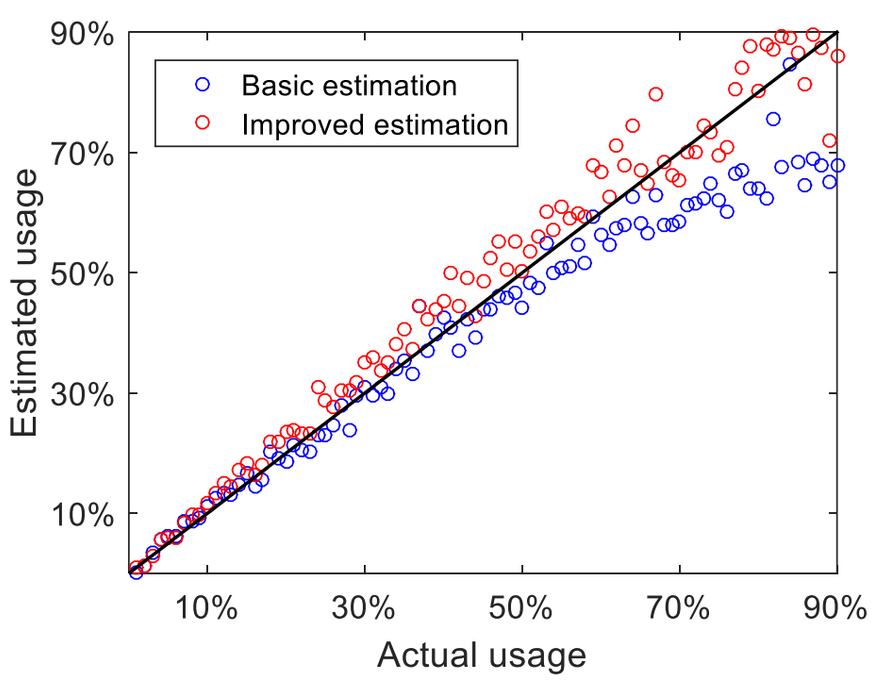


Classification Results





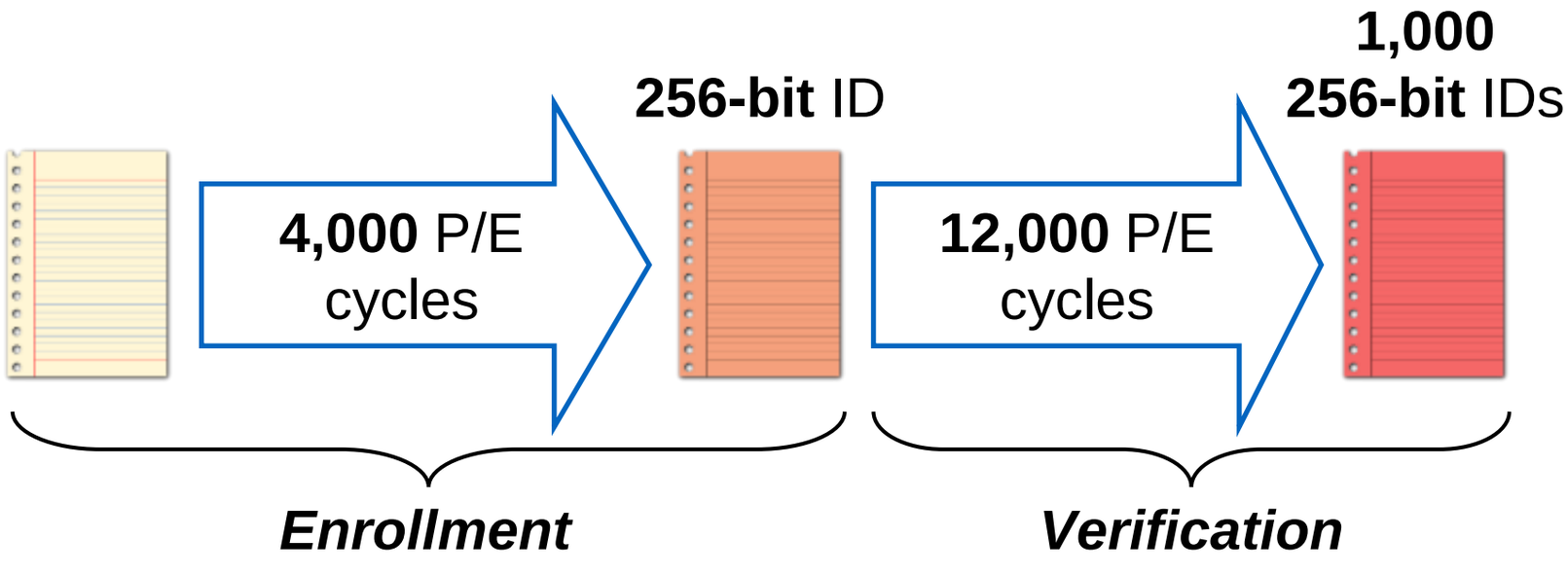




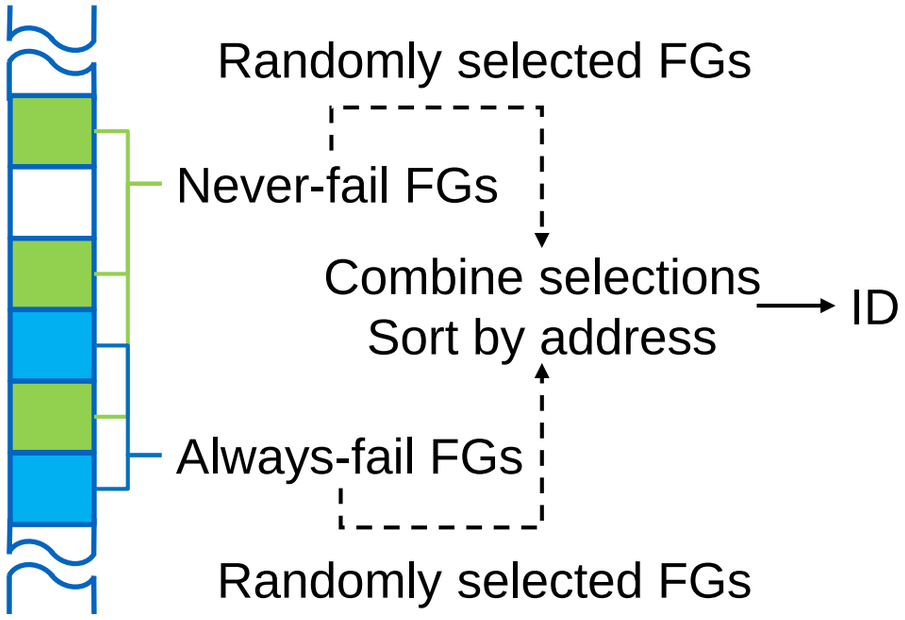
Source: Guo et al., DAC 2017

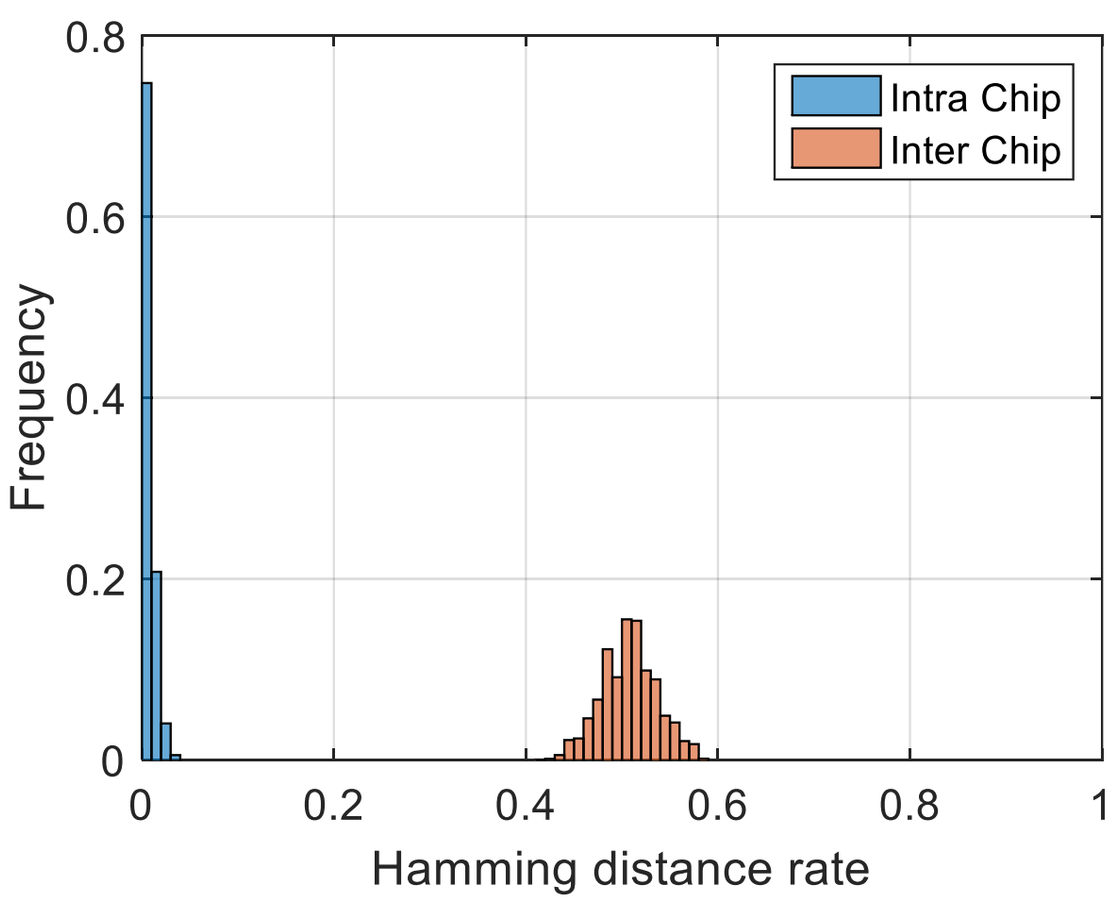
PUF (ID) Generation in Flash

Source: Guo et al., DAC 2017



- **Always-fail** FG transistors
- **Never-fail** FG transistors





Section VII.A: IP Encryption and IEEE P1735 Standard

ASIC Design Costs (2008)

- **Source:** http://chipdesignmag.com/display.php?articleId=1997
  - 180-nm averages $4 million in design costs
  - 130-nm averages $10 million in design costs.
  - 90-nm averages $25 million in design costs.
  - 45-nm design costs could be $50 million.
  - 32-nm design costs could be $75 million.

→ **Average chip designs are approaching the top prices of collectible, famous pieces of art (and that's just the design, not even the revenue!)**

Take inspiration companies that sell digital versions of valuable art i.e., add watermarks?

Semiconductor IP Watermarking

Signature of author → Binary sequence → Encryption → Conversion to watermark → Extract and verify

Main Features / Requirements

1) Functional Correctness
2) Minimal Overhead
3) Proof of Authorship
4) Persistence, i.e.,
   - Difficult to remove and/or modify
5) Invisibility

Watermarks are “passive”, i.e., do not prevent theft, overuse, reverse engineering, tampering, etc.

Need “active” methods such as hardware metering, obfuscation, and IP encryption

Purpose of P1735 Standard

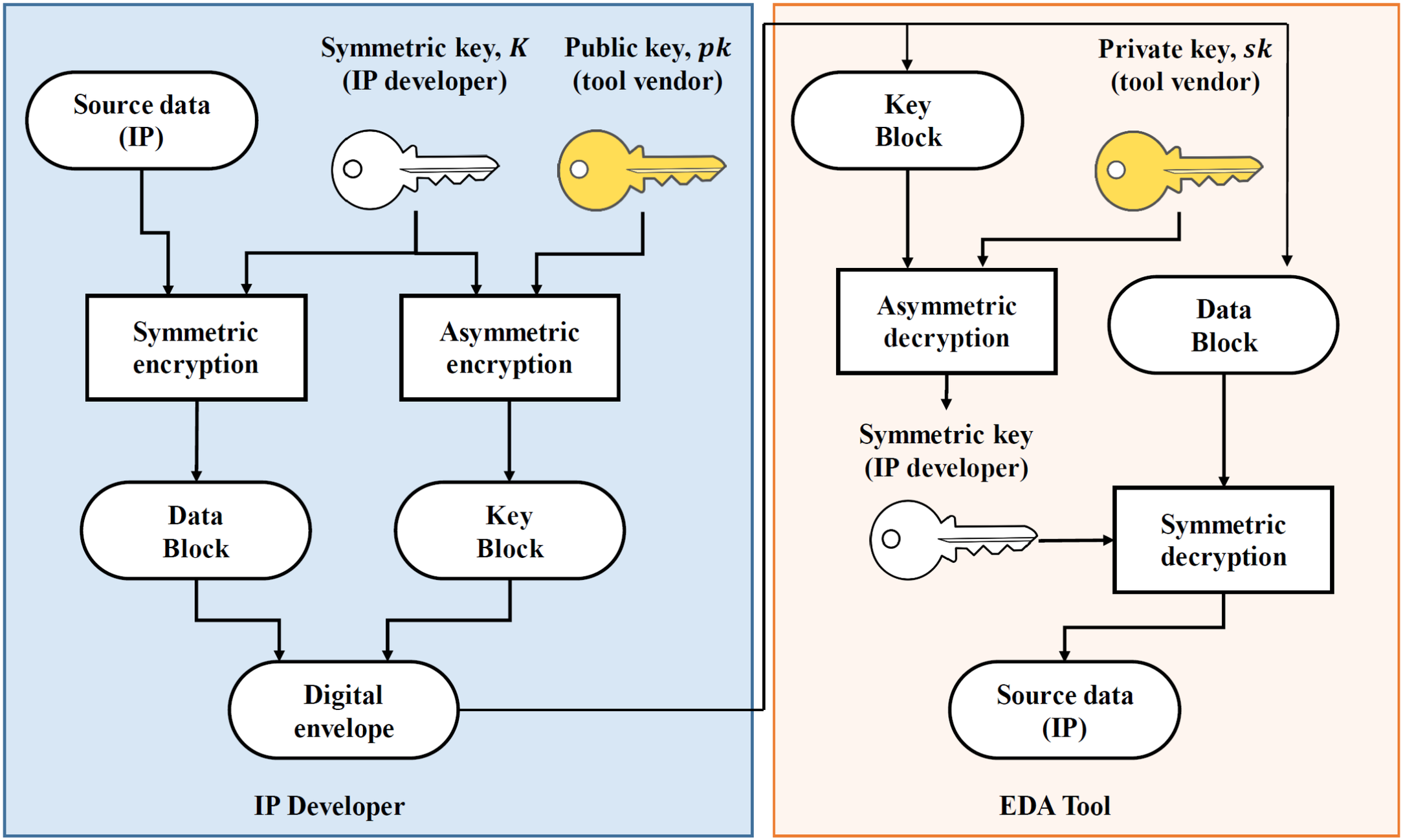
Control IP Pricing, i.e., *lower "risk premium" and increase "trust discount"*

Provide a uniform and interoperable standard to enable a design flow that

1) Aids IP authors in providing IP that can be processed by CAD/EDA tools without sharing protected information with IP users → ***Provide confidentiality*** ✗
2) Supports an integrated licensing scheme, enabling the IP authors to specify compile-time licenses → ***Provide access control*** ✗
3) Helps IP authors to control user rights including, but not limited to, IP visibility, allowed tool versions, and output file encryption → ***Maintain integrity of the above*** ✗

High Level View of IEEE P1735

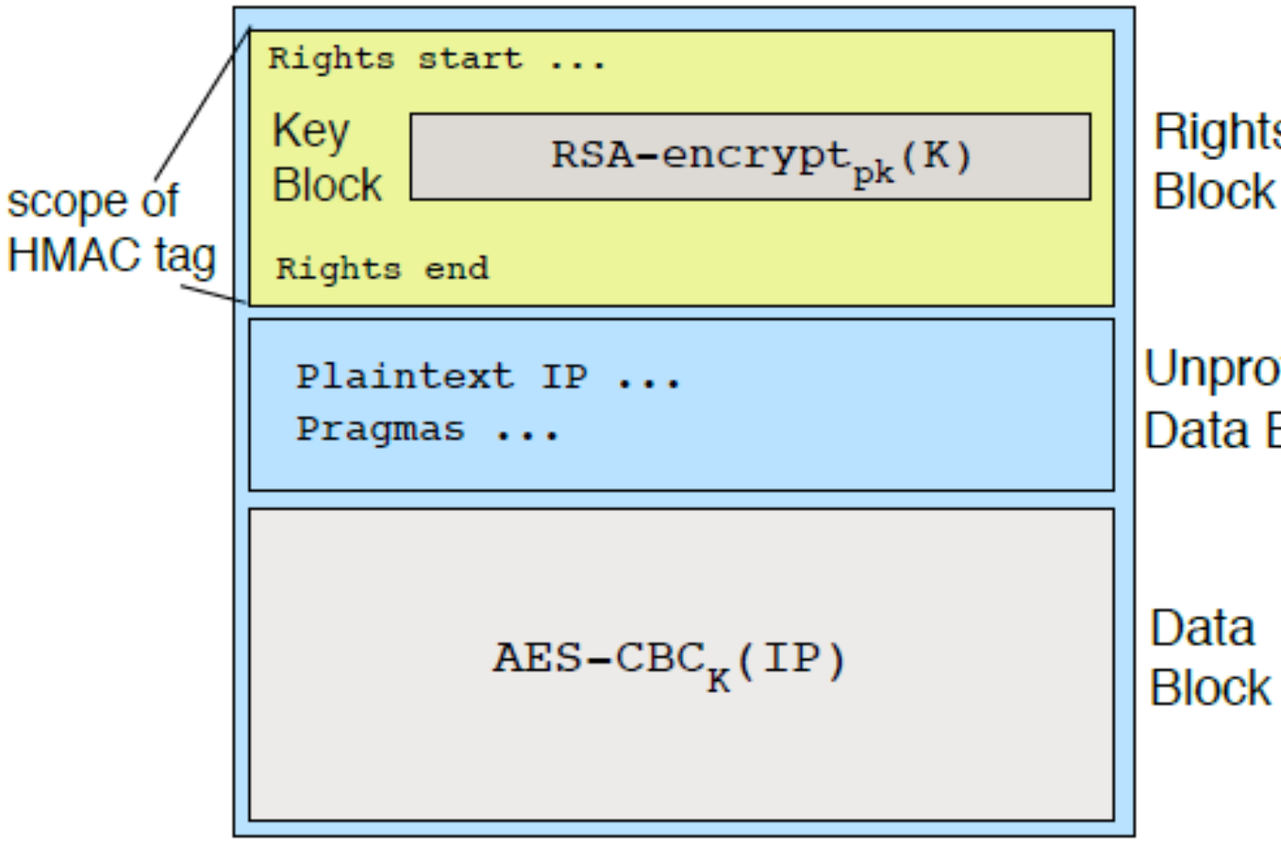
Source: Chhotaray et al, CCS, 2017



Assumption: EDA tool vendor is trusted

IP Encryption Example

Source: Chhotaray et al, CCS, 2017



Digital Envelope

```
`pragma protect key_keyowner="Synplicity",
`pragma protect key_block
cuwL7ZNavUR8d63+Ze2qh8SzxBnOw6brdyZMnGXzFz
/GqmrnecShDj/EXvQPw7dqfYcrhWd+V1LgDG7gHI/l
HMT5NsqBHA082CMLoVKrB0WoSOegOV4U+Xz2kn3h6X
fBR7ZHsTENT9ez2jBEBWwmzuf5DpfiayPX+pWQi8oq
EzcUfLbpuznT+YrxDrVXblxFKTrEjuNzArn51A==

`pragma protect encoding=(enctype="base64"
`pragma protect data_method="aes128-cbc"
`pragma protect data_block
7Qyfhub8J8jbYDPkgqKdd+Ni37SVLhTHucoUsWInQF
Vl/QeaTvNV69mli4CI7FCeDBgoprjkM=
`pragma protect end_protected

endmodule
```

Key Block → Session key

Data Block → Encrypted RTL code

Rights digest: A Hash-based Message Authentication Code (HMAC) generated to verify integrity of rights

IEEE P1735 Critique

Source: Chhotaray et al, CCS, 2017

1) Dictates that data block be encrypted with AES-CBC mode and padding scheme / error handling is undefined
   → **Padding oracle attack (POA)** is a well known weakness

2) Digest (HMAC) only covers the rights block
   → Data block can be tampered w/o detection or authenticity check

3) Consequences of syntax error visibility hand wavy
   → Critical information leakage

→ **Syntax oracle attack (SOA)**
→ **Hardware Trojan insertion and other modifications to IP**

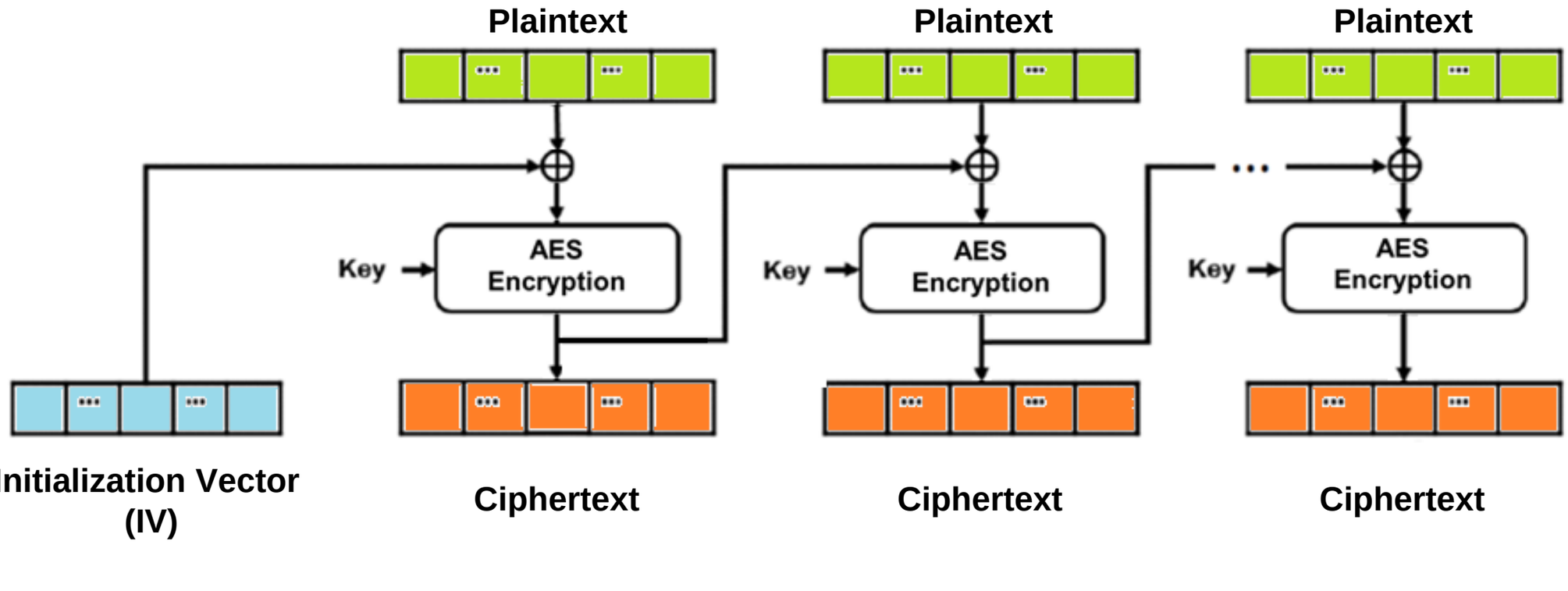
4) License verification protocol poorly defined
   → 'license deny" message can be changed to a 'license grant' message

5) Recommends PKCS#1 V1.5 padding scheme for RSA
   → Has been exploited as a side-channel to recover underlying plaintext (session key in P1735)

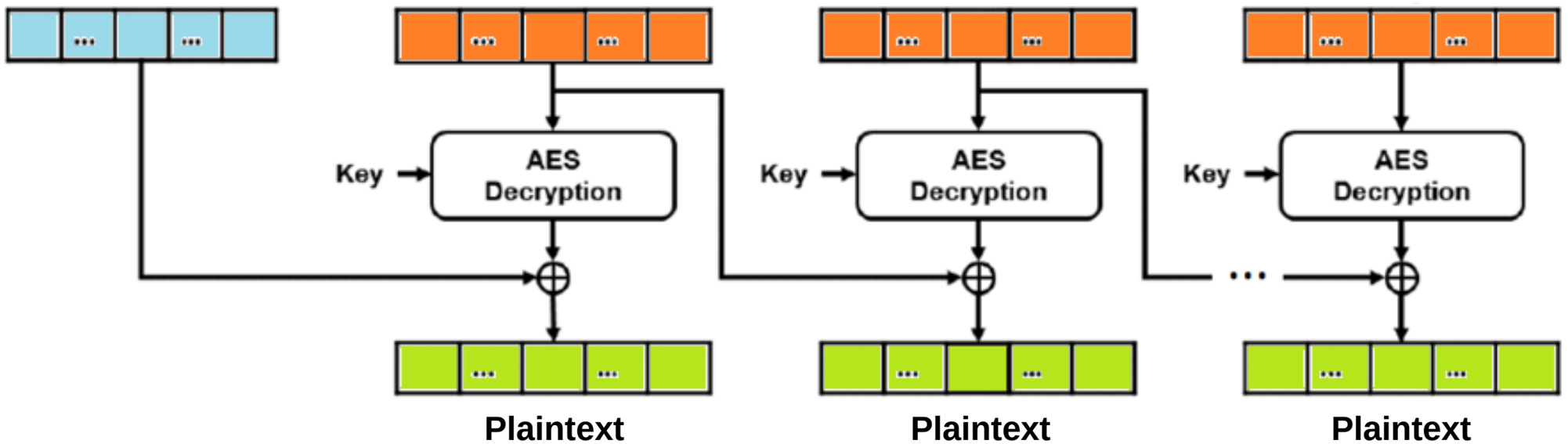
Not discussed here today

Cipher Block Chaining (CBC) Mode

CBC Mode Encryption



CBC Mode Decryption



PKCS#7 Padding

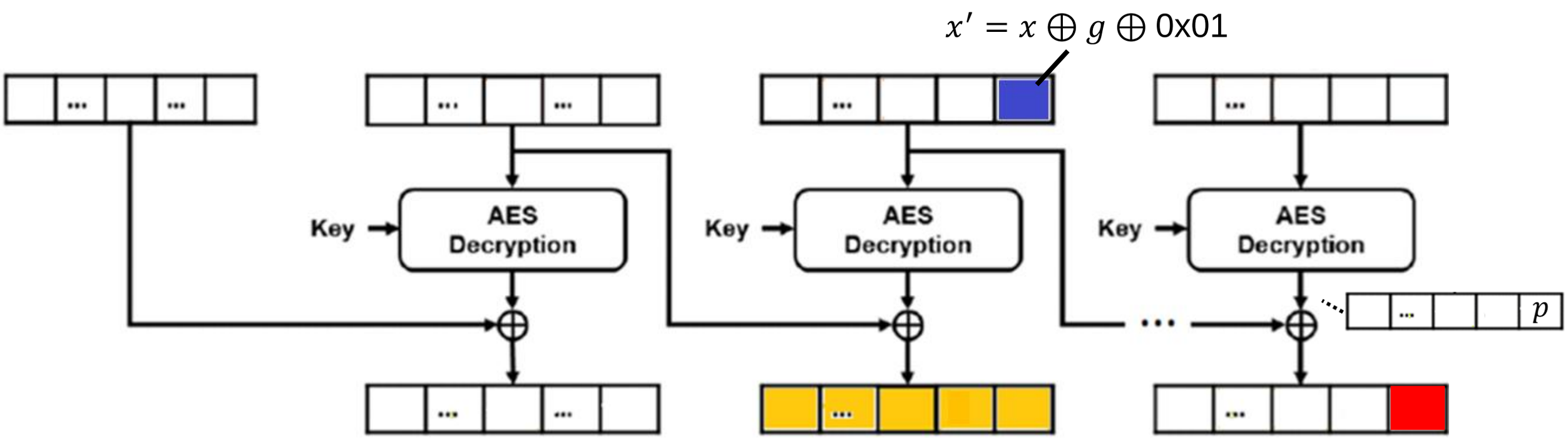
- Block ciphers require all blocks to be a specific length
  - Since plaintext messages come in a variety of lengths, padding is added to a plaintext block to increase its length to the required length
  - At least one padding byte is always appended

	1	2	3	4	5	6	7	8
w/out padding	‘A’	‘E’	‘I’	‘O’	‘U’	‘R’	‘S’	
w/ padding	‘A’	‘E’	‘I’	‘O’	‘U’	‘R’	‘S’	0x01
w/out padding	‘A’	‘B’	‘C’					
w/ padding	‘A’	‘B’	‘C’	0x05	0x05	0x05	0x05	0x05

- Final decrypted block should end with a single 0x01 byte (0x01), or two 0x02 bytes (0x02, 0x02), or three 0x03 bytes (0x03, 0x03, 0x03) and so on …
- If not, most cryptographic providers will throw an invalid padding error

Padding Oracle Attack (POA)

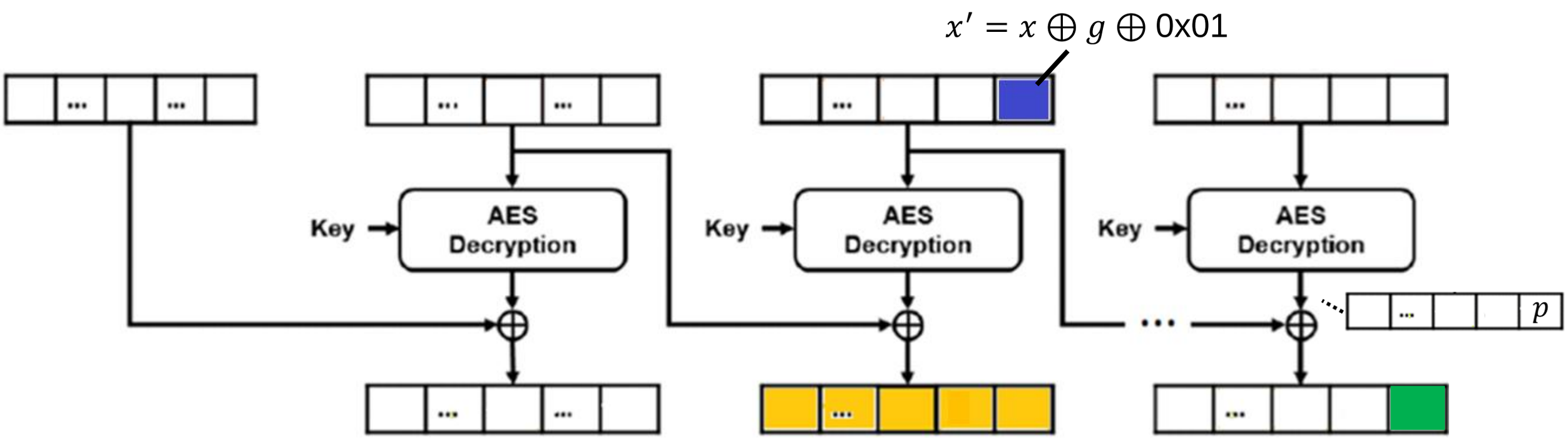
1) Adversary starts by guessing bytes in last block of ciphertext in reverse order. Last byte in prior block (x) is replaced by guess byte g XOR'd with x and padding byte (0x01).



Padding Oracle Attack (POA)

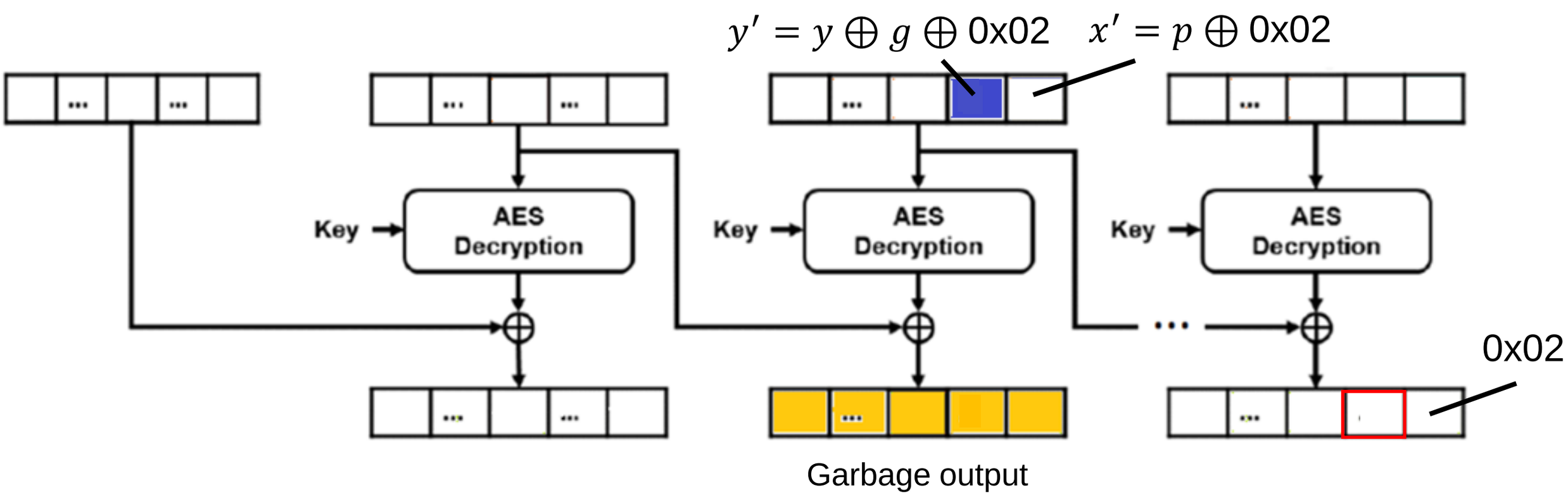
1) Adversary starts by guessing bytes in last block of ciphertext in reverse order. Last byte in prior block (x) is replaced by guess byte g XOR'd with x and padding byte (0x01).
2) Attacker repeats the process until an error is not thrown (i.e., original plaintext byte = g)

Note: Since there are only 256 possible values of a byte, the maximum number of guesses needed is 256



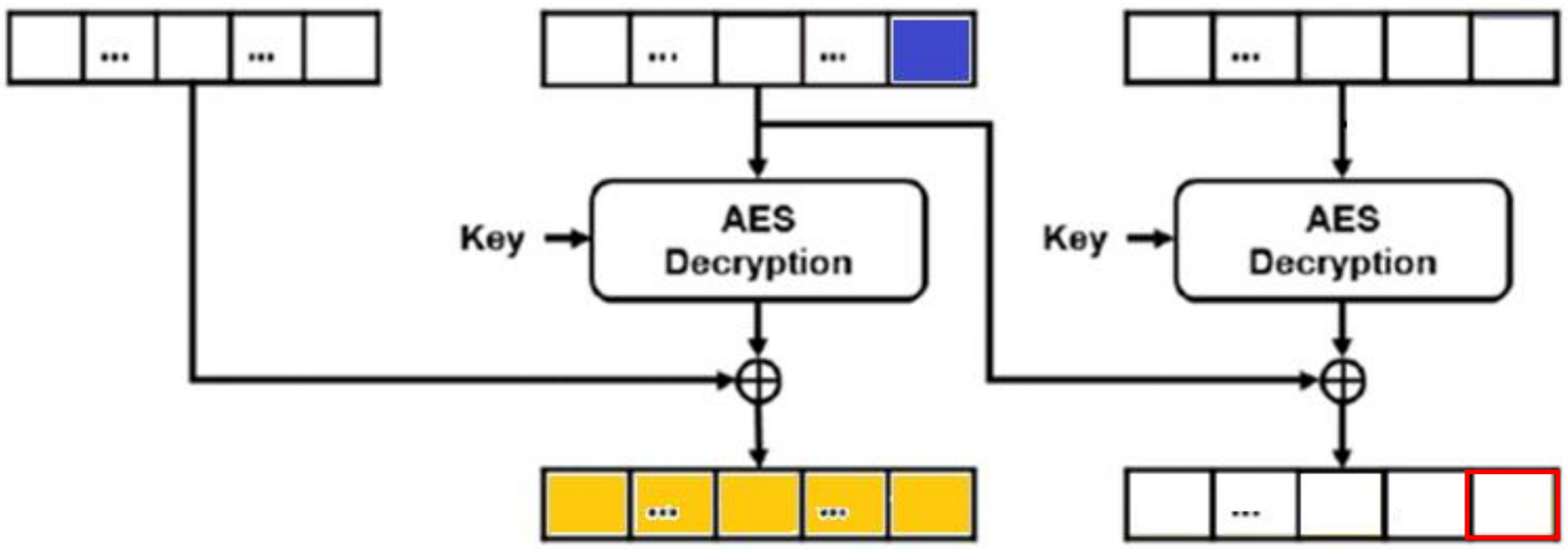
Padding Oracle Attack (POA)

1) Adversary starts by guessing bytes in last block of ciphertext in reverse order. Last byte in prior block (x) is replaced by guess byte g XOR'd with x and padding byte (0x01).
2) Attacker repeats the process until an error is not thrown (i.e., original plaintext byte = g)
3) Attacker moves onto 15th byte and uses padding byte (0x02), and so on



Padding Oracle Attack (POA)

1) Adversary starts by guessing bytes in last block of ciphertext in reverse order. Last byte in prior block (x) is replaced by guess byte g XOR'd with x and padding byte (0x01).
2) Attacker repeats the process until an error is not thrown (i.e., original plaintext byte = g)
3) Attacker moves onto 15th byte and uses padding byte (0x02), and so on
4) When the block is finished, attacker removes it and repeats the process

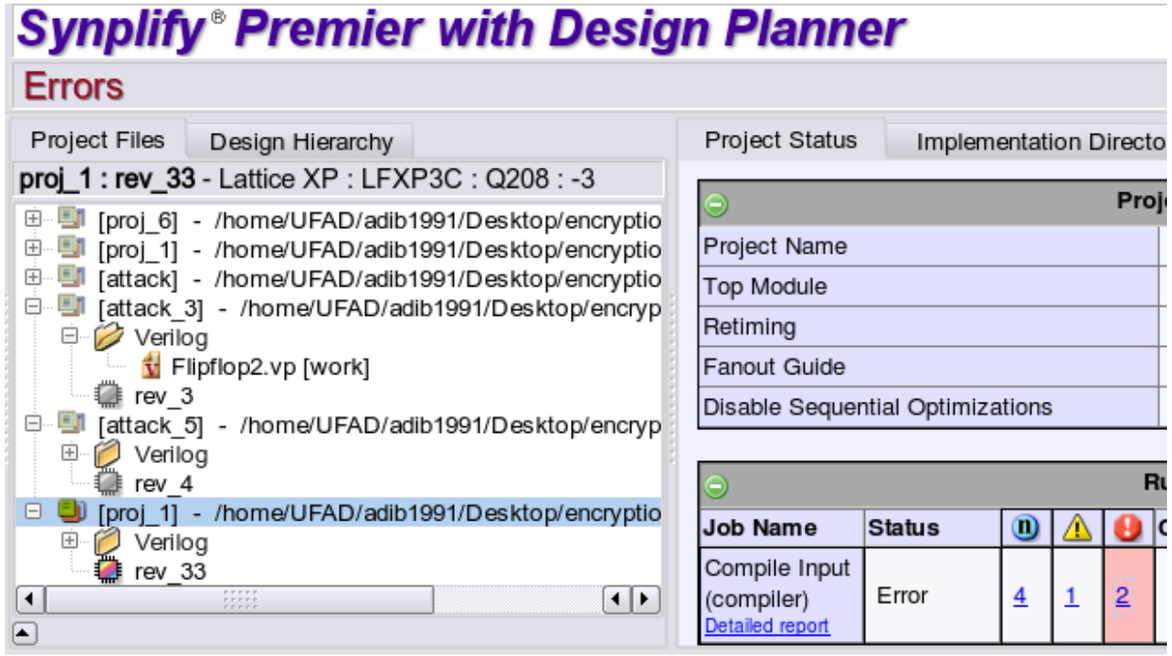


Garbage output

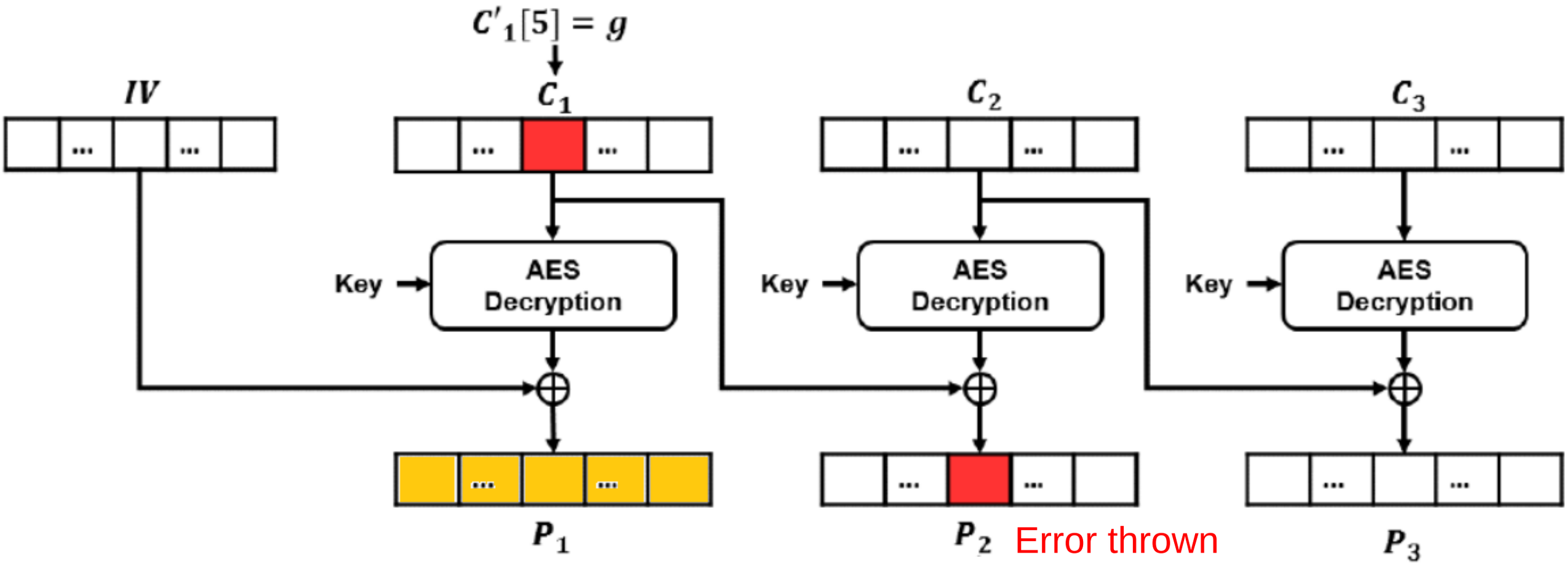
Syntax Oracle Attack (SOA)

Differences from POA

- A character that causes a **unique syntax error** (`) is introduced instead of padding byte
- When the unique error is observed from the tool, the plaintext byte can be recovered
- Does not have to proceed backwards and is **highly parallelizable** (all blocks simultaneously in extreme case!
- However, there are cases where the syntax error (`) is masked so **some plaintext cannot be recovered directly from the attack**



SOA Illustrated



Garbage output

Note: Errors masked if garbage output produces certain characters (e.g., EOF)

Attack Optimizations

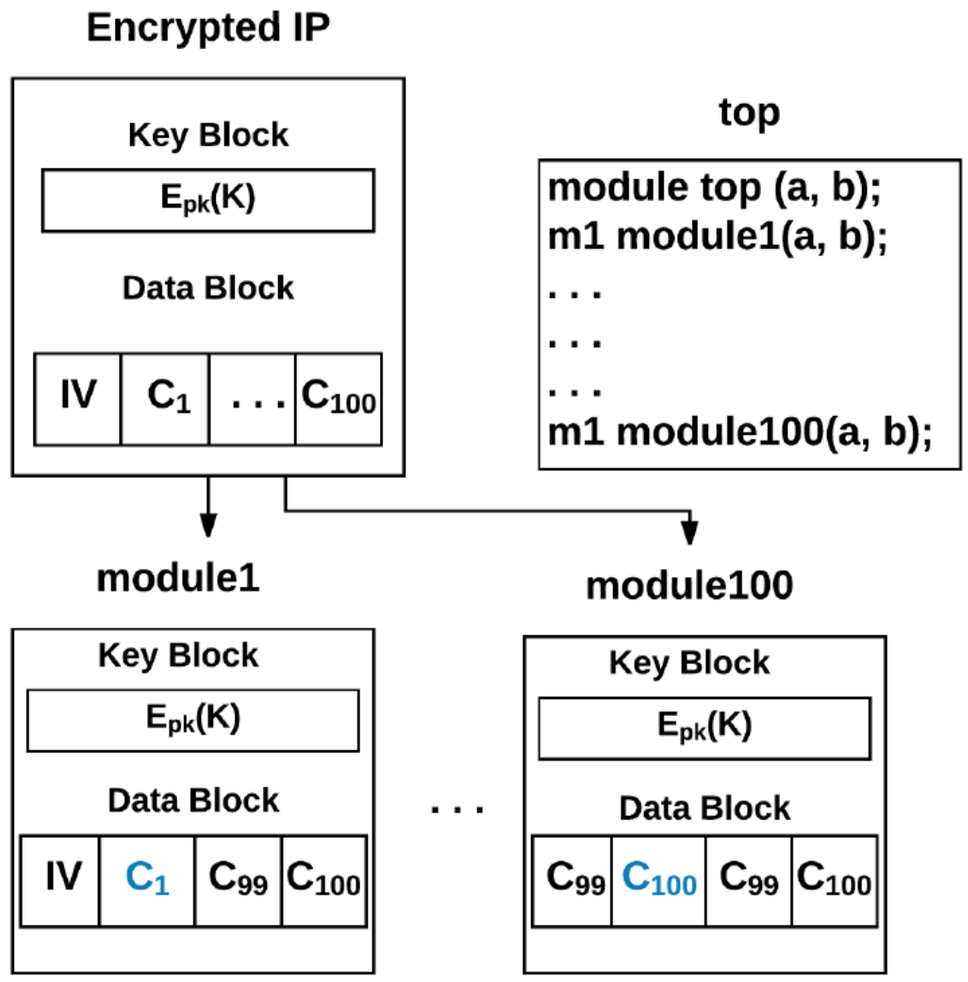
Applicable to POA and SOA

1) Reduce sample space of guess byte (RSSGB)
   - Reduces maximum number of attempts per guess from 256 to 128 (# of ASCII characters)
2) Reducing AES decryptions (RAD)
   - Reduces complexity from $O(N^2)$ to $O(N)$

Recover rate: ~1300 blocks/hour

Applicable to SOA only

3) All-blocks-at-once attack (ABAO)
   - Reduces maximum number of AES operations to $128 \times N$



All-blocks-at-once attack (ABAO)

SOA-ABAO can recover IP 10x times faster than POA with > 85% accuracy

Source: Chhotaray et al, CCS, 2017

Recommended Fixes

Simple Fixes for POA

- Change the padding scheme to one that has no invalid padding
- Change to AES-CTR (i.e., counter) mode, which does not require padding of the plaintext

Complex Fixes Required for SOA

- Apply an authenticated encryption (AE) scheme → simultaneously provides confidentiality, integrity, and authenticity assurances on the data
  - Encrypt-then-MAC, Encrypt-and-MAC, MAC-then-Encrypt
- Same fix should also prevent hardware Trojan insertion

Section VII.B FORTIS for End-to-End Protection of New IC Designs and IP

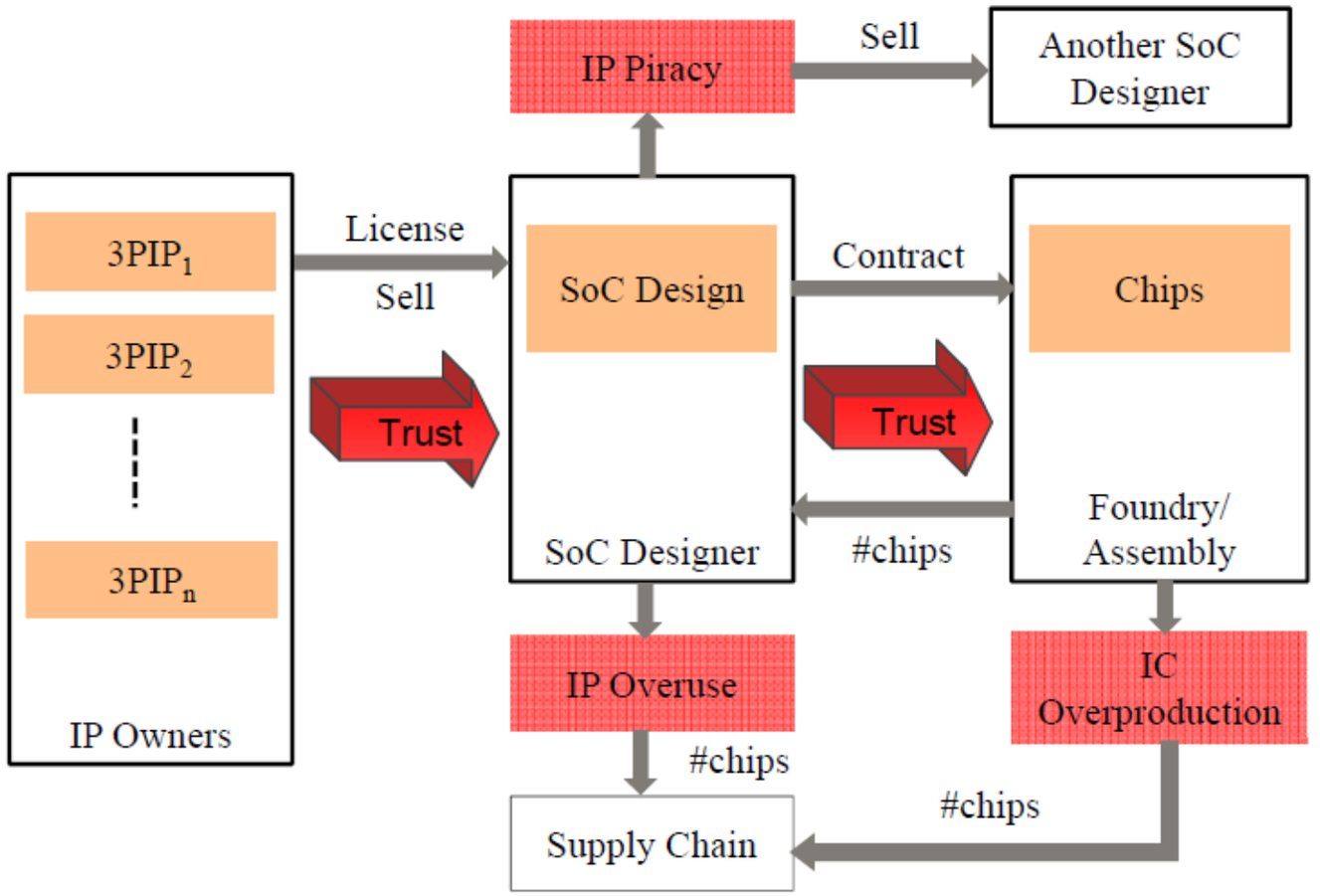
What is Forward Trust?

IP Trust must exist in 'backward' direction of supply chain

- Can SoC designer trust that 3PIP does not contain a hardware Trojan or malicious backdoor?
- Can consumer/ design house trust that IC/IP does not contain a hardware Trojan or malicious backdoor?

'Forward' trust must also exist from (1) IP overuse; (2) IP piracy; and/or (3) IC overproduction

- IP owners to SoC designers
- IP owners to foundry
- SoC designers to foundry
- SoC designers to assembly



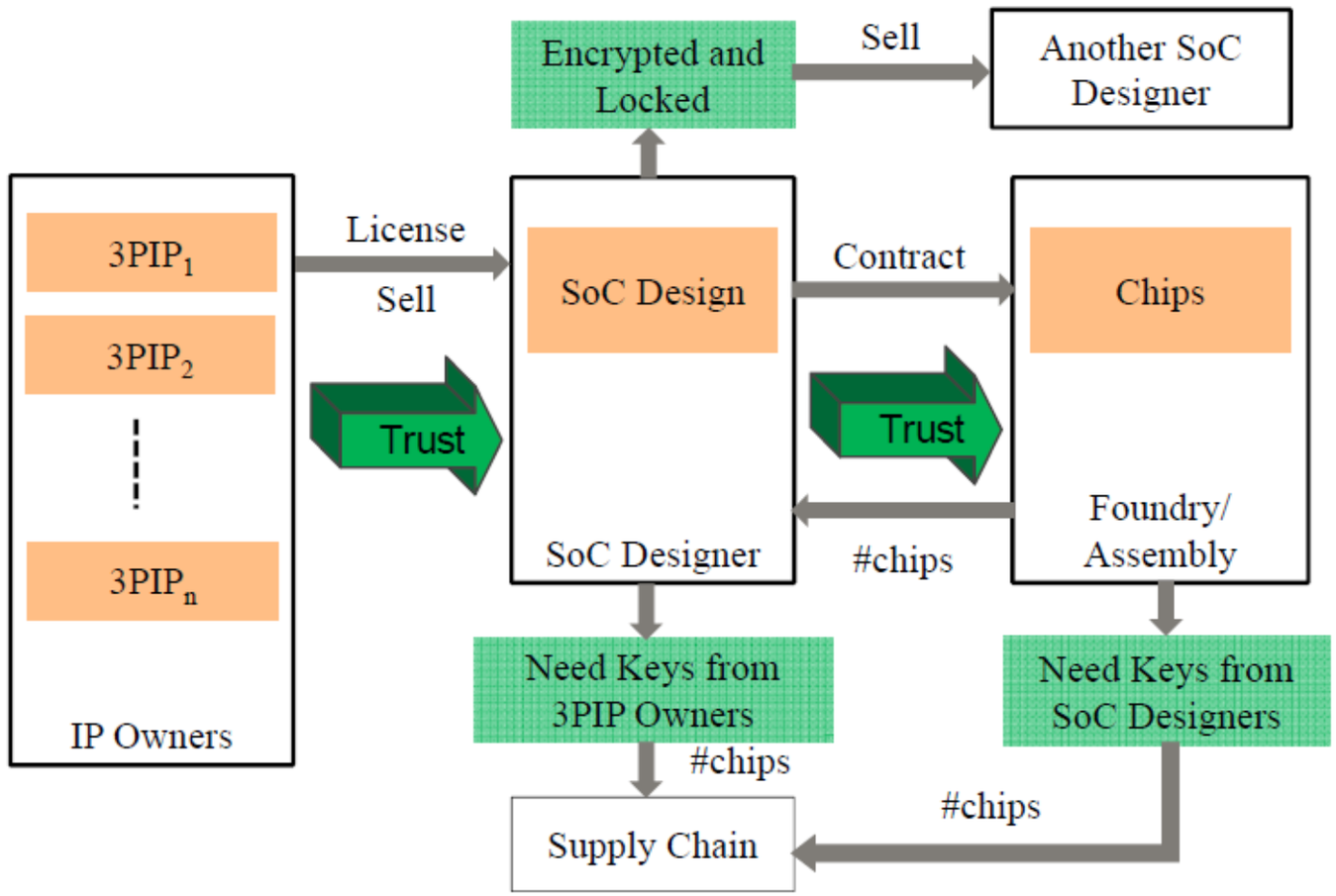
Source: Guin et al, TODAES, 2016

FORTIS Overview

Main components

1) Logic Locking
2) Netlist Encryption (following P1735 standard)
3) IP Digest (or AEAD)

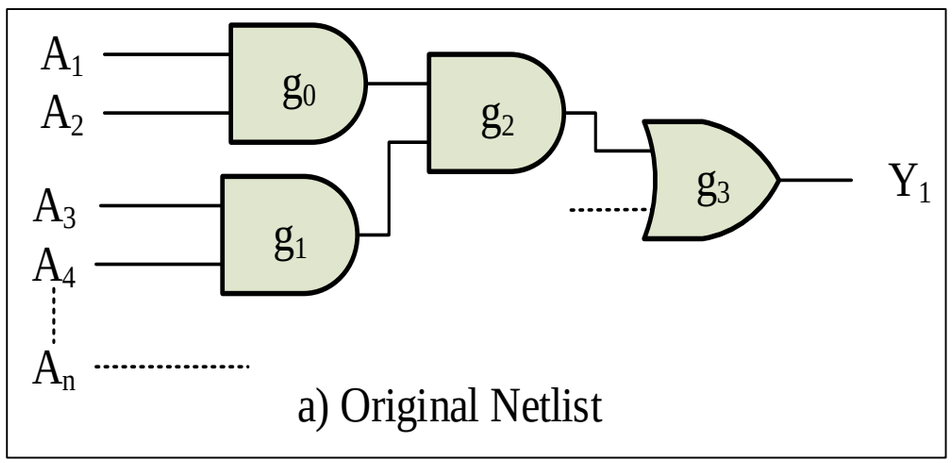
Source: Guin et al, TODAES, 2016



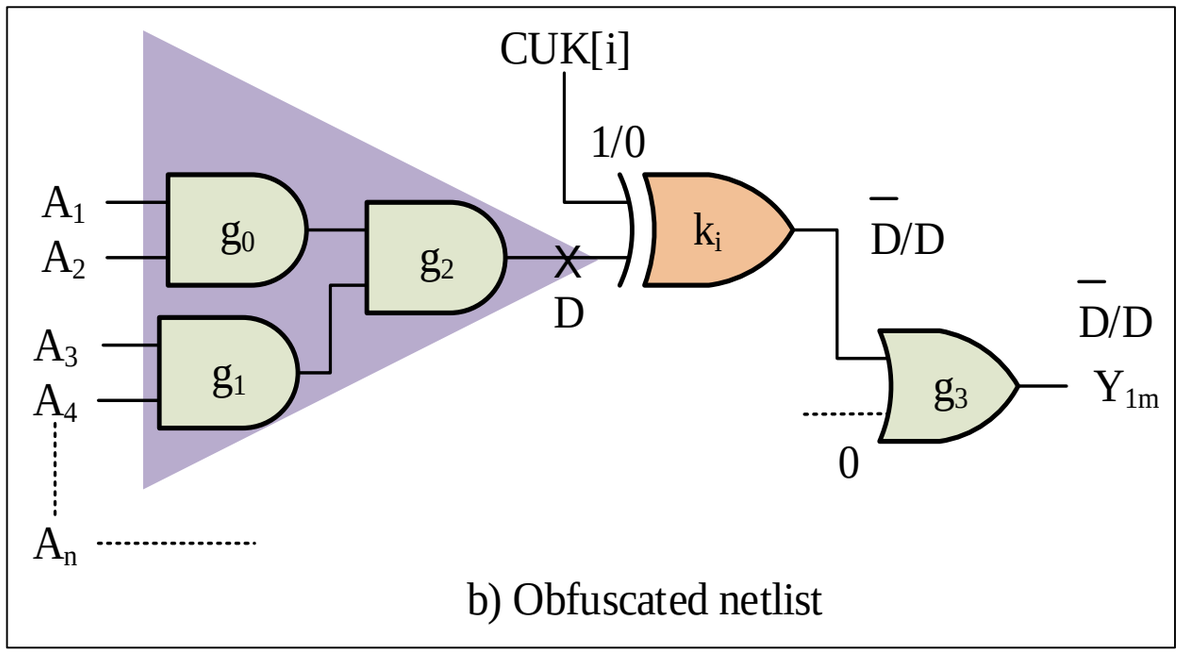
- Steps 2+3 protects confidentiality and integrity of IP
- Step 1 provides metering ability to prevent IC overproduction and IP overuse (also requires on-chip key exchange hardware)

Logic Obfuscation/Locking

Roy et al., DATE 2008



Source: Guin et al, TODAES 2016

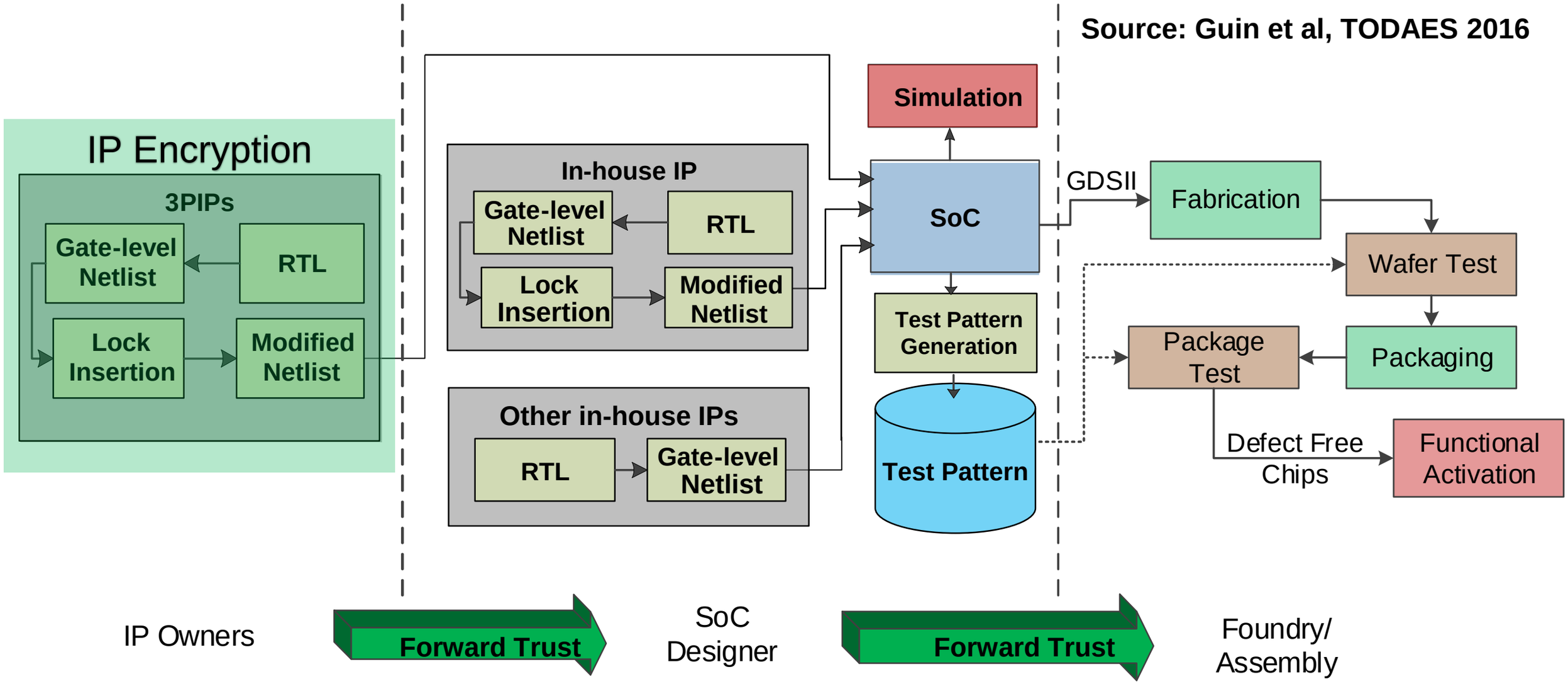


Placement of key gates

- Should produce adequate corruptibility from original netlist
- Should not be placed in timing critical paths
- Should not be easily removed, bypassed, etc. to recover original design
- Should not be easy to recover key even when a working chip is available to attacker [1, 2]

[1] El Massad et al., NDSS 2015
[2] Subramanyan et al, HOST 2015

FORTIS Design, Fabrication, and Test

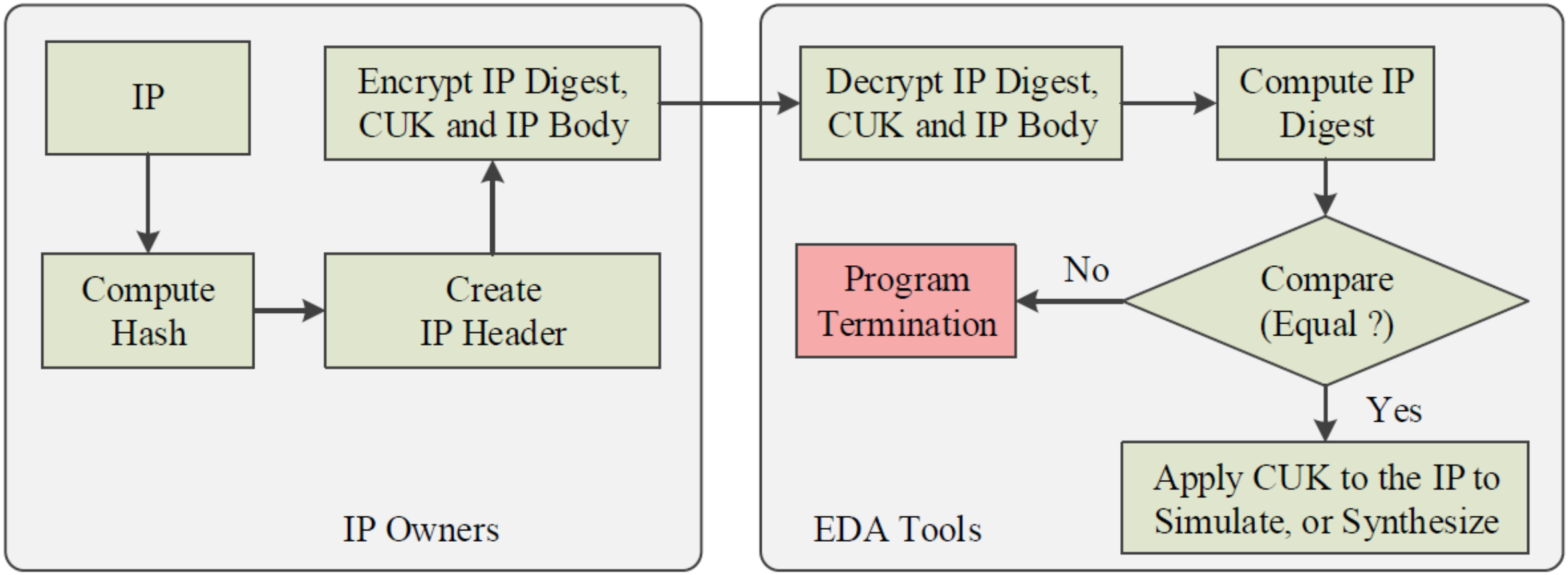


3PIP owner provides

(1) Locked, but synthesizable RTL or gate level netlist with confidentiality and integrity protected by IEEE P1735 to SoC designer (*does not contain unlocking key or CUK)

(2) An unlocked RTL or gate level netlist with confidentiality and synthesis rights protected by IEEE P1735 to SoC designer's EDA tool

FORTIS Digest and Check

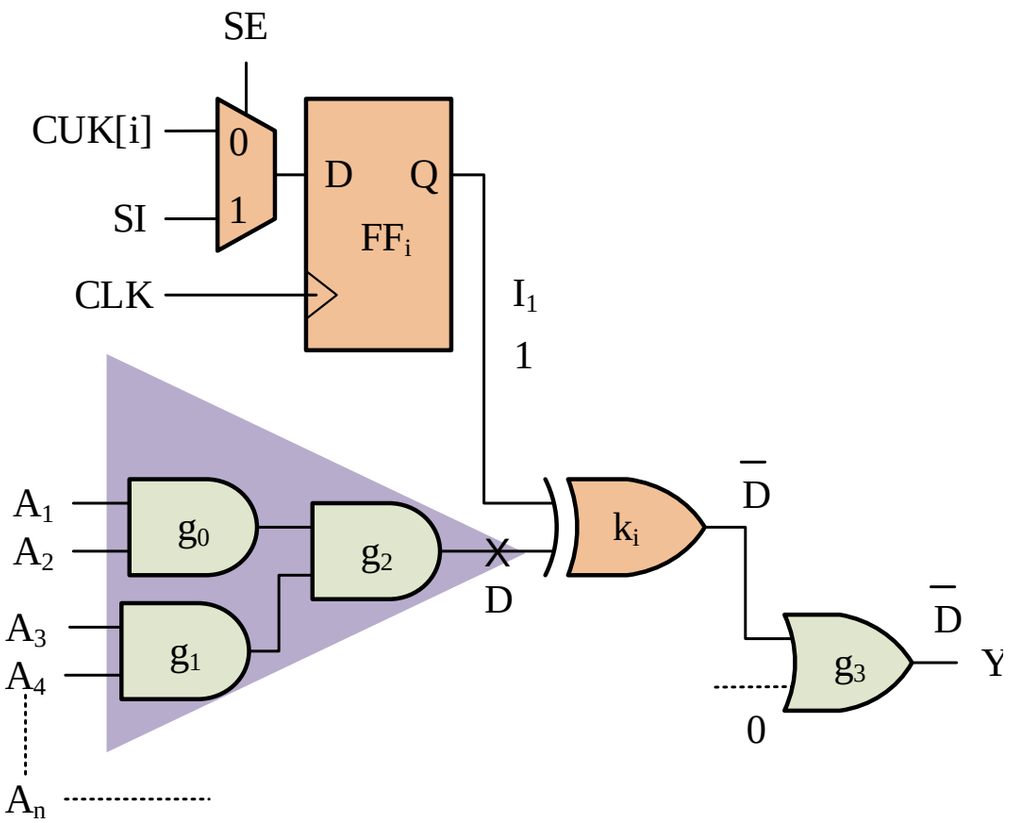


Source: Guin et al, TODAES 2016

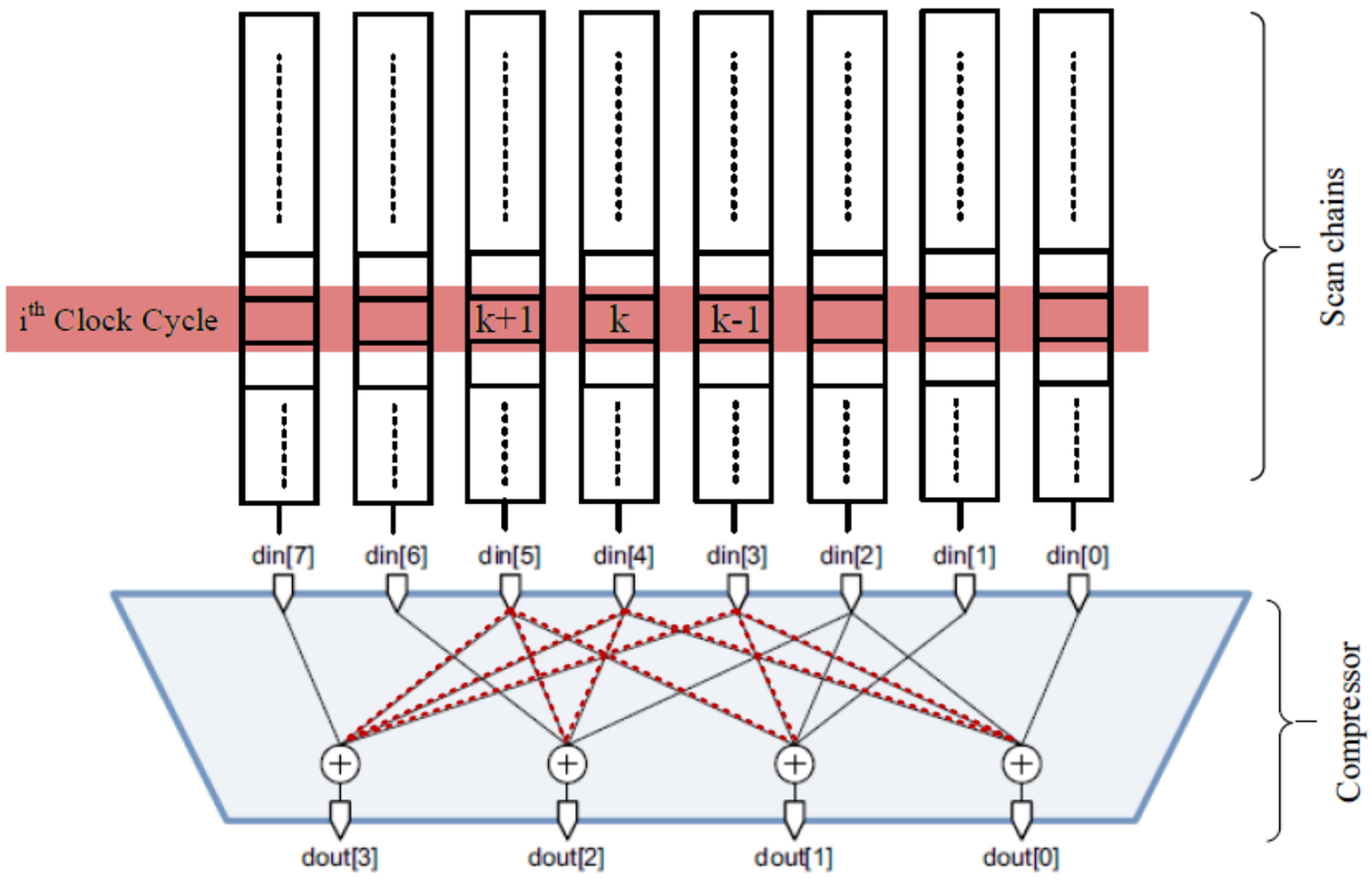
- IP digest = hash of entire locked netlist (including declarations, etc.)
- IP header contains (1) chip unlock key (CUK) to unlock chip for simulation and or post-fabrication and (2) calculated digest
- EDA tool will terminate if digest doesn't match (i.e., IP was modified)

Wafer and Package Test

- Use flip flop outputs as key inputs
- Provide foundry/assembly with any incorrect key during testing
- Utilize the inherent obscurity provided by the scan compression

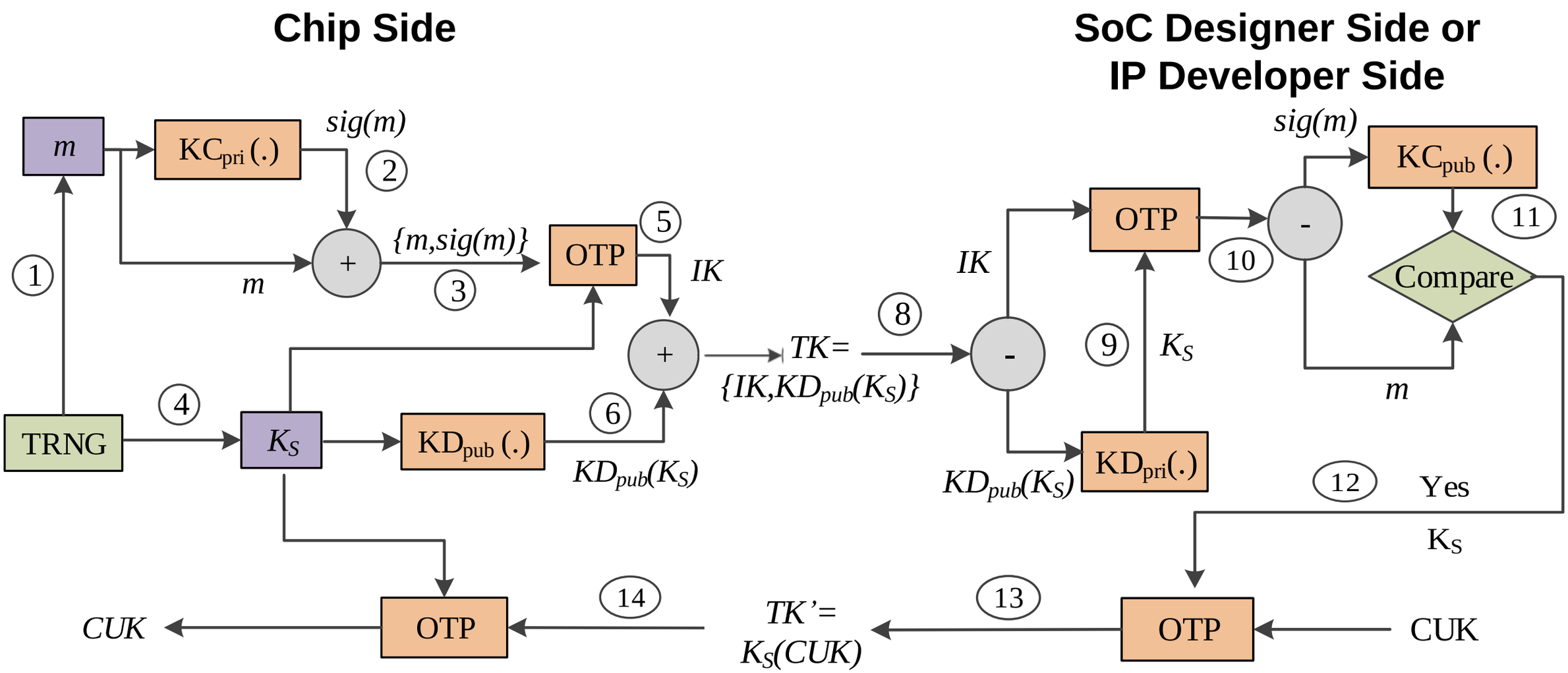


c) Proposed Netlist



Source: Guin et al, TODAES 2016

CUK Exchange Protocol



Source: Guin et al, TODAES 2016

- **Based on PGP [1]:** Provides message integrity, endpoint authentication, and confidentiality
- **Like SST**, avoids cloning, overproduction, and out-of-spec/defective ICs

[1] Zimmermann, MIT Press 1995

FORTIS Results and Future Work

Experimental Results

- Little to no impact on test coverage
- Low area overhead

Limitations and Future Work

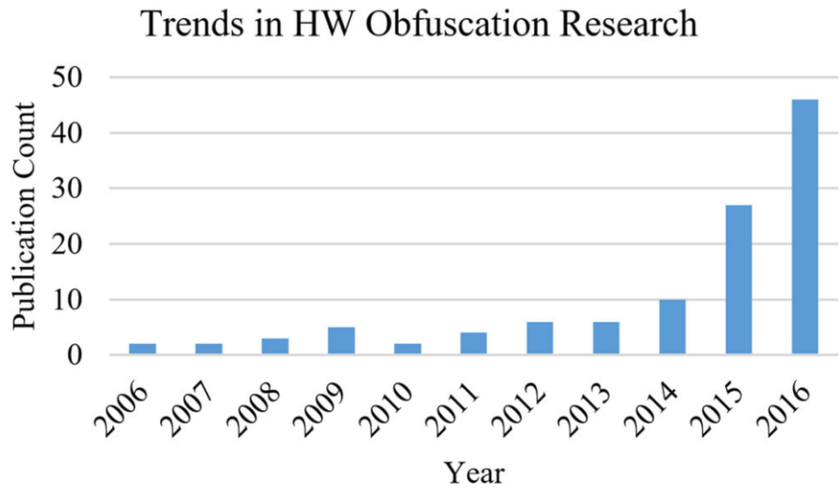
- **P1735 Revision**
- **Attacks Against Logic Obfuscation**
  - Several attacks e.g., key sensitization attack, SAT based attacks have been proposed to break logic obfuscation
  - By protecting scan chain, SAT attacks can be avoided, but originally proposed scan compression approach can be bypassed

Section VIII: Open Problems and Future Research Directions

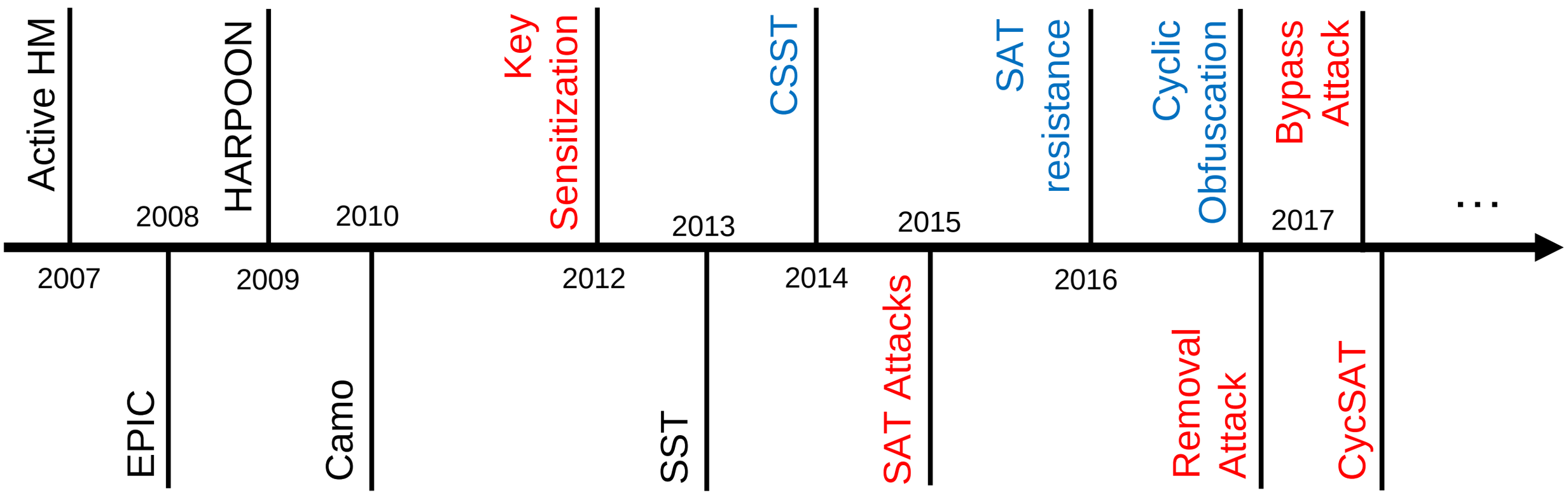
The Need for Formal Treatments

HW Obfuscation (logic locking, FSM, camo) → an ongoing game of cat-and-mouse

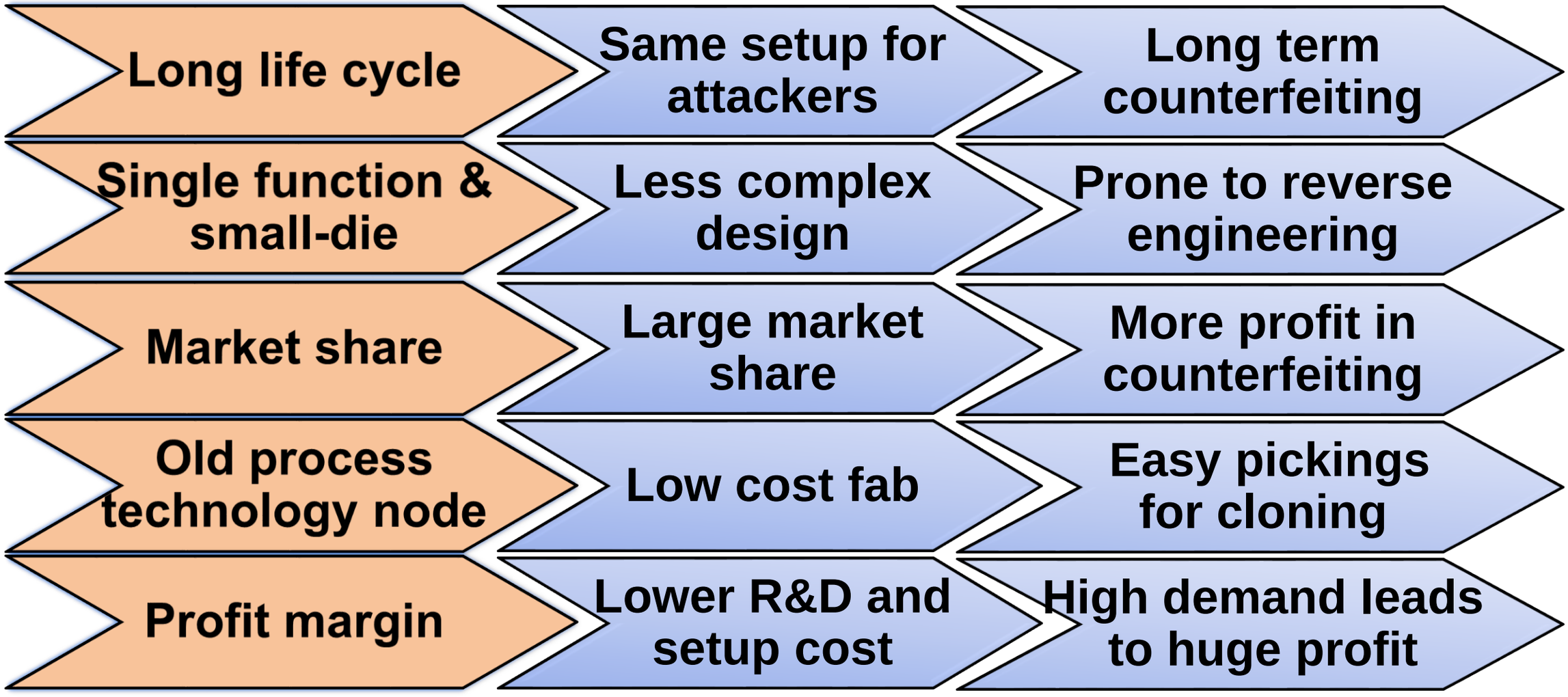
Image: economist.com



Source: Amir et al., HaSS 2018



AMS Counterfeit Detection & Avoidance



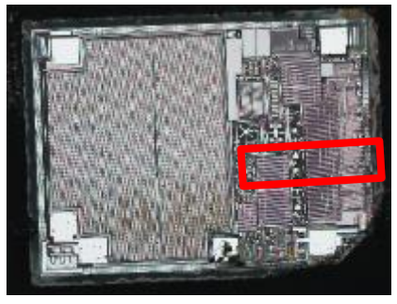
Types of AMS Counterfeits

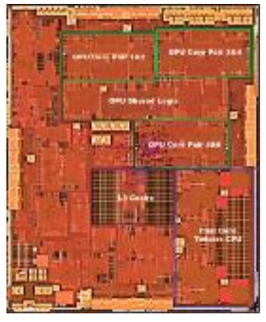
- Recycled, Remarked, Overproduced, Cloned
- Out-of-spec/defective and tampered less likely

Differences between AMS and Digital

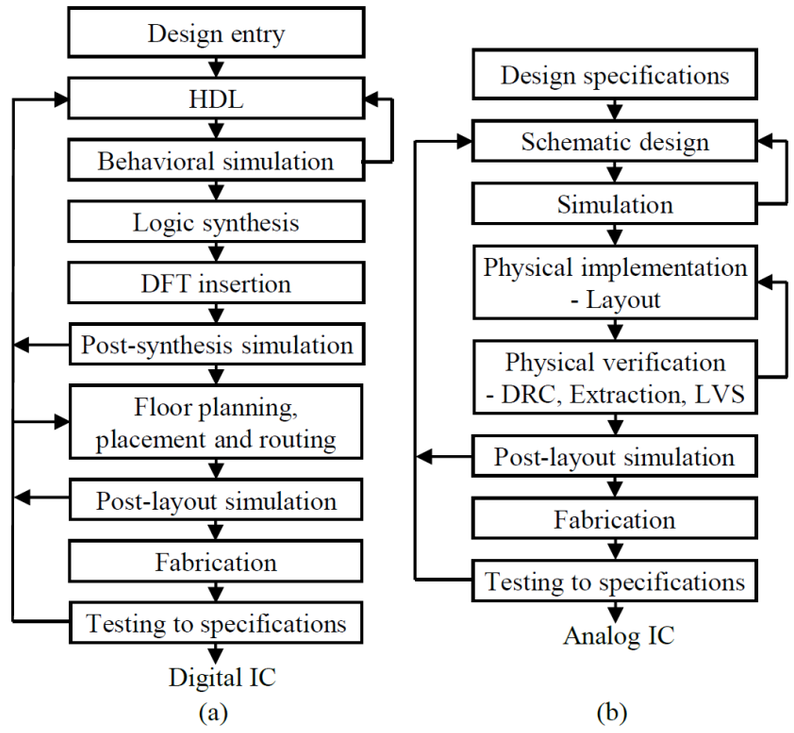
1. **Pin Count:** Digital ICs contain ten to several hundred pins; AMS ICs have less than ten to one hundred

2. **Complexity/Cost:** AMS ICs are fabricated with older technology nodes (e.g., 180nm), have lower transistor counts (< hundred in many cases), and fewer metal layers (<3); some may cost pennies





3. **Design, Test, and Verification Flows:** AMS requires greater precision in biasing conditions, sensitivity to noise and temperature, and emphasis on signal integrity; tighter design margins; simultaneous considerations of multiple parameters
4. **Missing in Action (MIA):** Many common elements of digital chips are limited or nonexistent in AMS (memories, pipelines, crypto, modulo arithmetic, error correction...)



M. Alam et al., HASS 2017

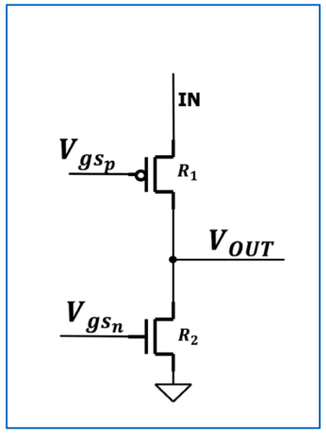
Consequences and Challenges

Attacks and countermeasures for counterfeit, anti-reverse engineering, etc. have been aimed primarily at digital circuits

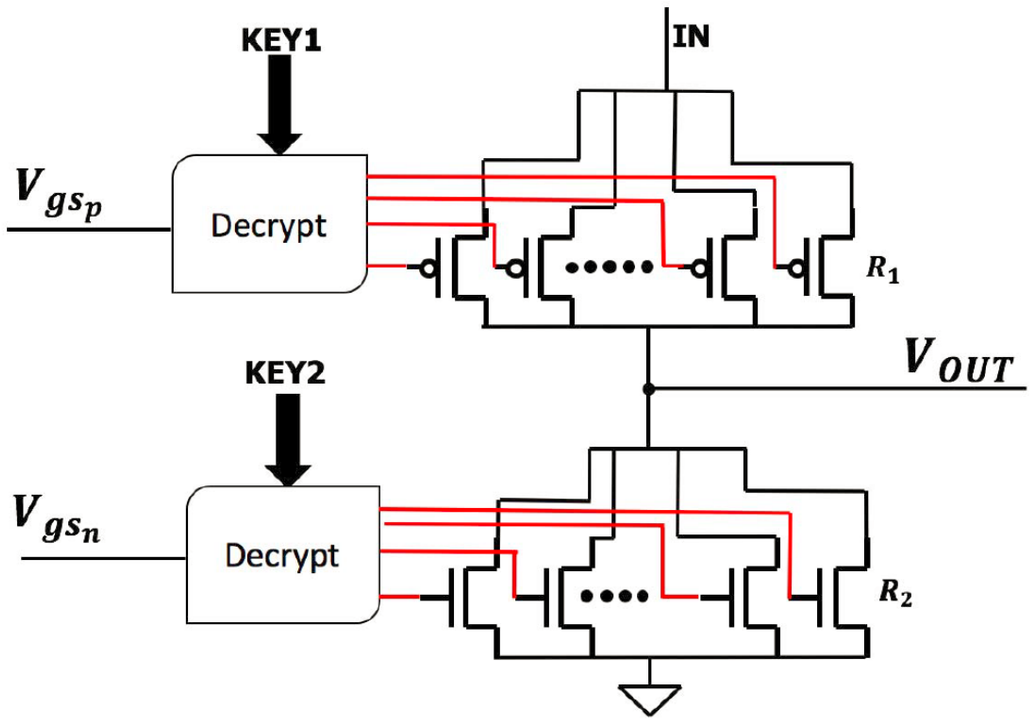
	The Bad	The Good
Low pin count	PUF, CDIR, etc. access limited	-
Lesser process variations	PUF quality impacted?	-
Lack of combinational/ sequential logic	No crypto for remote communication with chip; obfuscation and locking unsuitable	SAT and scan chain based attacks not applicable
Limited test infrastructure	Internal access limits counterfeit detection	Internal access limits black box attacks

Analog Metering

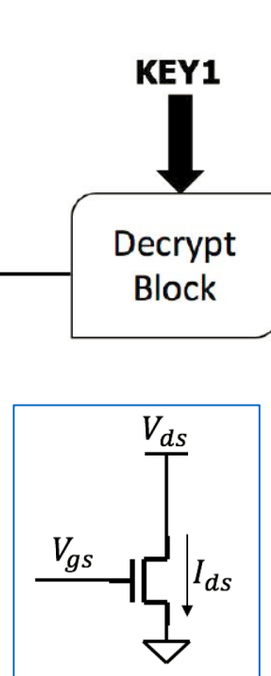
Source: Rao et al., LATS 2017



Voltage Biasing Circuit



Obfuscated Voltage Biasing Circuit



Current Biasing Circuit

Obfuscated Current Biasing Circuit

Summary of Challenges

- Breakable by spec analysis of experienced analog designer
- Obfuscation (anti-RE) not addressed
- Impact of process variations on corruptibility
- Key initialization/storage mechanisms still vague

Legacy Devices with Obsolete Components

Best Approaches

- Design with maintenance in mind
  - Well-documented
  - Platform independent SW/RTL
- Life-of-type (LOT) buys

Critical Infrastructures

Military

Financial

Civil

Medical

Limited Remaining Options

1) Same Obsolete HW/SW

- Expensive if purchased through authorized distributors
- Untrustworthy if purchased through unauthorized distributors
- Loss of HW/SW support/patches

2) Replace with new HW/SW

- Backwards compatibility issues
- Compliance and recertification

Upgrade/Downgrade Framework

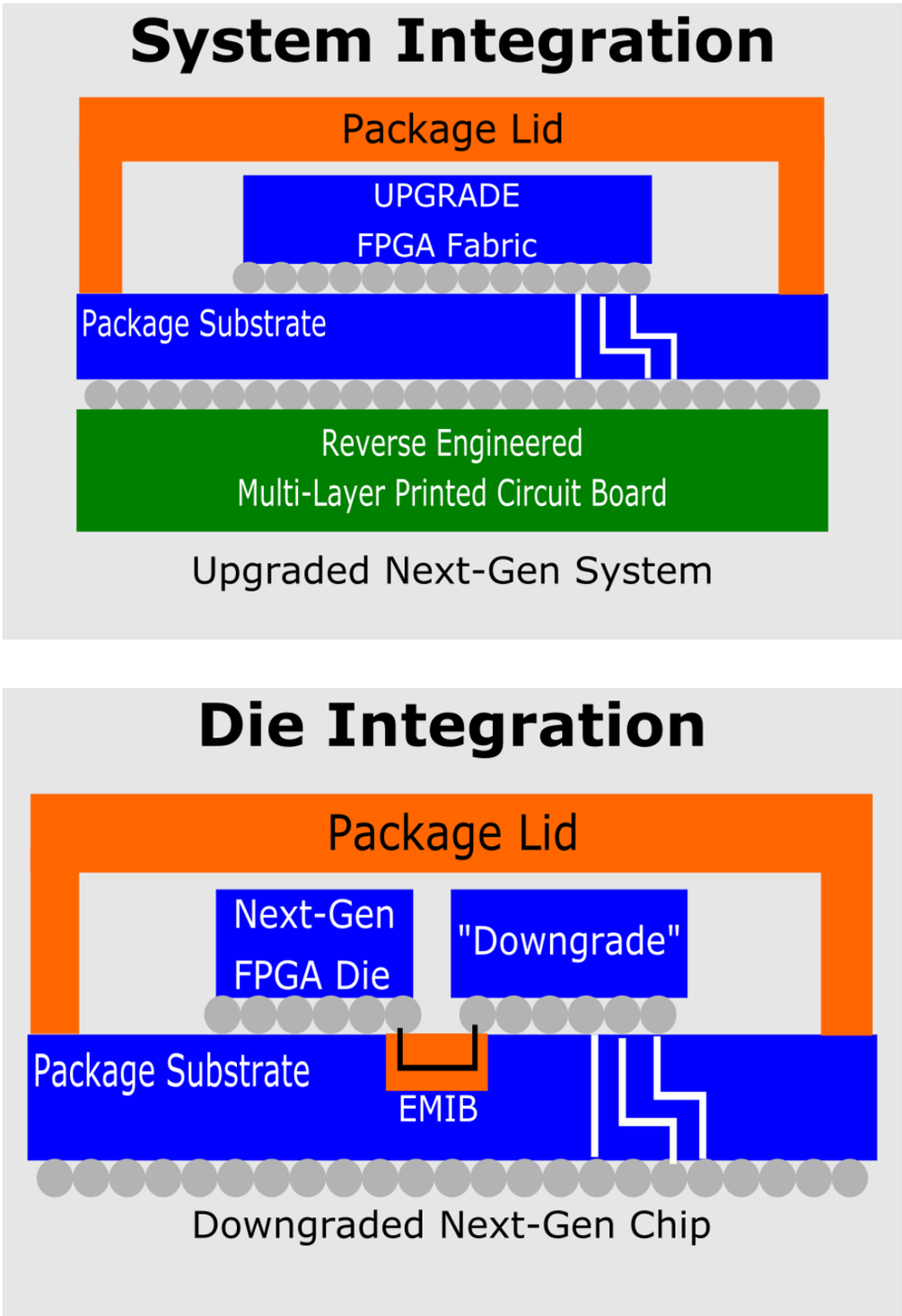
Source: Botero et al., IEEE D&T 2018 (in press)

Upgrade: *"Raising to a higher standard, in particular improve by adding or replacing components."*

- Develop a reconfigurable fabric with digital, analog, and mixed signal blocks to replace the legacy system
- Emphasis on improvements to security, footprint, performance, etc. compared with the legacy system

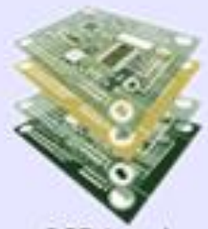
Downgrade: *"Reduce to a lower grade, rank, or level of importance."*

- Convert a next-generation die into a backwards compatible chip by integrating with "downgrade" die using advances in packaging
- Emphasis on maintaining same security, footprint, performance, etc. compared to obsolete chip

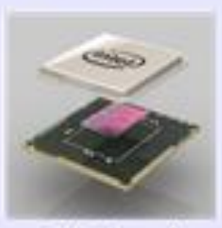


Proposed Steps and Recommendations

Reverse Engineering



PCB Level



Chip Level

Software / Firmware Level

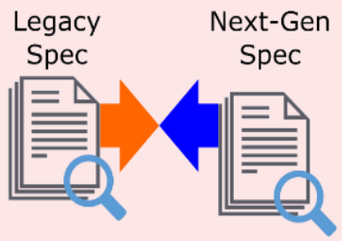
System / Component Profiling

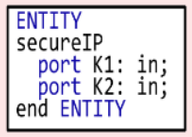
Reliability

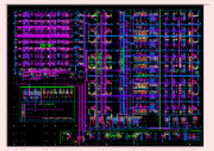
Performance

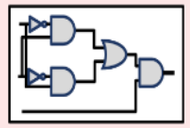
Security

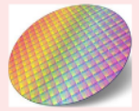
Mapping



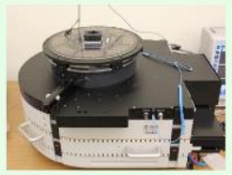








Validation & Verification



Desiderata

Cost-effective / Efficient

Automated

Non-destructive

Compliant

Recommendations for Realization

- Automation in RE @ all levels (IC, PCB, FW, SW)
- Security assessment tools and property-driven hardware security
- Commodification of mapping platforms
- Machine learning for specification mining, system verification, compliance checks

Section IX: Conclusion

Summary – Counterfeit Detection

	Recycled	Remarked	Overproduced	Out-of-Spec/ Defective	Cloned	Tampered
Discrete	Physical Inspection	Electrical Tests	Physical Inspection		Electrical Tests	Reverse Engineering	Physical Inspection / Reverse Engineering
SoCs, uPs, etc.				Electrical Tests		
Memories		Adv. Elec. Tests		Electrical Tests		
FPGAs		Adv. Elec. Tests		Electrical Tests		
AMS				Electrical Tests		
PCB				Electrical Tests		

- No one-size fits all solution!
- Physical inspection and/or reverse engineering can be improved in terms of time, cost, accuracy, etc.
- Electrical testing can be improved for out-of-spec/defective detection of larger digital chips
- Gaps in recycled AMS and SoCs, uPs, etc. detection

Key

N/A
Good
Needs Improvement
Unexplored or inadequate

Summary – Counterfeit/Piracy Avoidance

	Recycled	Remarked	Overproduced	Out-of-Spec/ Defective	Cloned	Tampered
Discrete	F-CDIR	PUF				
SoCs, uPs, etc.	CDIR	ECID, PUF	FORTIS, HM, SST	SST	FORTIS, HM, SST, camo	Strong PUF; BISA; Split Manufacturing. OBISA
Memories	CDIR	ECID, PUF	FORTIS, HM, SST	SST	FORTIS, HM, SST, camo	
FPGAs	CDIR	ECID, PUF	FORTIS, HM, SST	SST	FORTIS, HM, SST, camo	
AMS	F-CDIR	ECID? PUF	HM?		Obfuscation?	PUF?
PCB					Obfuscation	PUF?; Split Manufacturing

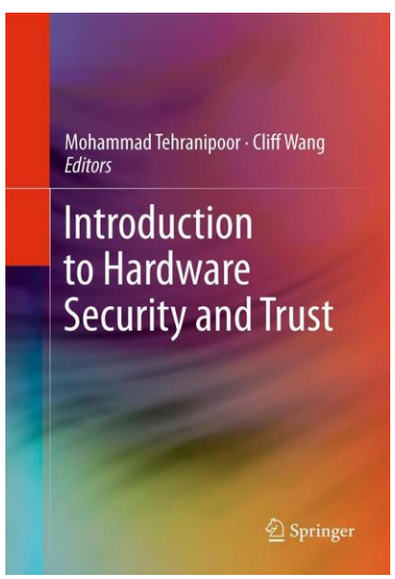
- No one-size fits all solution!
- Recycled, remarked, and tampered probably addressed if technologies are adopted
- FORTIS, HM, SST, camo, etc. need formal treatments, revisions, and adoption
- Gaps in AMS, PCB, and discrete

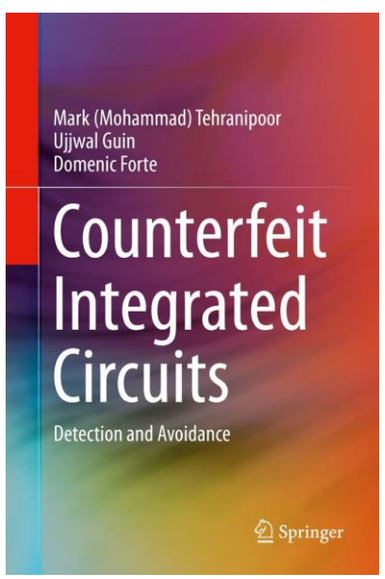
Key

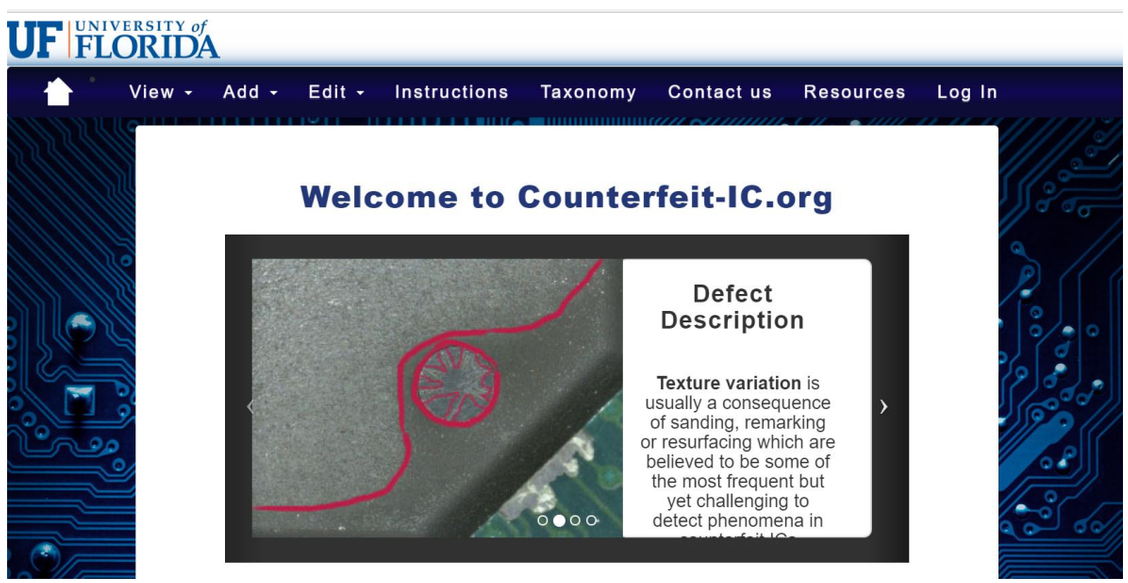
N/A
Good
Needs Improvement
Unexplored or inadequate

Conclusion

More resources on these topics …







Thoughts and questions