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).

<table>
<thead>
<tr>
<th>Top Part Type Reported in Counterfeit Incidents</th>
<th>Where Used</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Industrial Market</td>
</tr>
<tr>
<td>Analog IC</td>
<td>14%</td>
</tr>
<tr>
<td>Microprocessor IC</td>
<td>4%</td>
</tr>
<tr>
<td>Memory IC</td>
<td>3%</td>
</tr>
<tr>
<td>Programmable Logic IC</td>
<td>30%</td>
</tr>
<tr>
<td>Transistor</td>
<td>22%</td>
</tr>
</tbody>
</table>

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.
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?

### States of Existence
- **Obsolete**
- **Active**
- **New**

### Analog and Mixed
- Transistors, diodes
- Amplifiers
- ADCs, DACs
- Mixers, etc.

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

#### Counterfeit by production status
- Active: 10%
- NRFND: 10%
- EOL: 4%
- Discontinued: 17%
- Transferred: 14%

#### Counterfeit report by device type
- Memory ICs: 18%
- Programmable logic ICs: 4%
- μPs/Peripheral: 2%
- Amplifiers: 5%
- Telecoms: 6%
- Transistors: 10%
- Diodes: 10%
- Logic ICs: 14%
- Optoelectronics: 14%
- Misc.

Source: IHS, 2016

Legacy systems are most heavily impacted - incentive

AMS most widely reported FPGAs and memories on the rise
Counterfeit Cisco Routers (2010)

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

Xilinx vs. Flextronics (2013)

- Quote for 50k components for Airvana: $X*50k ($X/part)
- Quote for 40k components for Checkpoint: $Y*50k ($Y/part, $X < $Y)
- Purchase 50k components ‘for Airvana’

Xilinx preferred customer (Airvana)

- Request 10k components: $X*10k
- 10k parts @ $X*10k

Flextronics

- Request 40k components
- 40k parts $Y*40k

Other customer (Checkpoint)
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)

- 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)

- 30 fake Apple stores found in Shenzhen
- Even employees were fooled
- “Apple Store” written on signs
Section II: Adversarial Models and Counterfeit Taxonomies
Globalization became essential to reducing design and fab costs.
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)

Remove Next Layer

Image Layer with SEM

Extract IC Netlist

Chipjuice

Pix2Net

Automated Plasma FIB Backside
(Principe et al., ISTFA 2017)

Backside 5 Axis Milling

varioMill

Backside Image Layer with SEM

Remove Next Layer

Image Layer with SEM

TESCAN FERA FIB-SEM
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

- **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.

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

Source: Tehranipoor et al., Springer, 2015
Mech./Env. Defect Taxonomies

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

Proc./Elec. Defect Taxonomies

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

- **Physical Inspections**
  - **Incoming Inspection**
    - Low Power Visual Inspection
    - X-Ray Imaging
  - **Exterior Tests**
    - Blacktop Testing
    - Microblast Analysis
    - Package Config. and dimension Analysis
    - Hermeticity Testing
    - Scanning Acoustic Microscopy (SAM)
    - Scanning Electron Microscopy (SEM)
  - **Interior Tests**
    - Optical Inspection
    - Wire Pull
    - Die Shear (Hermetic Devices)
    - Ball Shear
    - Scanning Acoustic Microscopy (SAM)
    - Scanning Electron Microscopy (SEM)
  - **Material Analysis**
    - X-Ray Fluorescence (XRF)
    - Fourier Transform Infrared Spec. (FTIR)
    - Ion Chromatography (IO)
    - Raman Spectroscopy
    - Energy Dispersive Spectroscopy (EDS)

- **Electrical Inspections**
  - Parametric Tests
  - Functional Tests
  - Burn-In Tests
  - Structural Tests

- **Aging-Based Fingerprints**
  - Early Failure Rate (EFR)
  - Path-Delay Analysis

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

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

Source: Tehranipoor et al., Springer, 2015
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


Counterfeit Incidents Reported

25% annual growth rate

Source: IHS, 2011

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

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

---

**WIRE BOND**
- Mold Compound
- Die
- Die Attach
- Wire Bond
- Solder Ball
- Rigid Laminate Substrate

**FLIP CHIP**
- Epoxy Underfill
- Die
- Mold Cap

Source: pcmag.com
Low-Power Visual Inspection (LPVI)

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

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

Ghost markings
Heat sink mark indicating prior usage
Peeled off lead plating
Residual material indicates reworking

Source: Honeywell

Common imaging method
**X-Ray ‘Nondestructive’ Imaging**

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

**Common imaging methods**

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

**Traditional Bond Pull Test**

![Image of traditional bond pull test](Source: xyztec.com)

**Virtual Bond Pull Test**

![Image of virtual bond pull test](Source: xyztec.com)

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

![Image of different die and lead frame](Source: ISTFA 2014)

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

![Image of broken bond wires](Source: ISTFA 2014)

**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)

Change in erase time in Macron Flash (150nm)

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

Common imaging method

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

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

- 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

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

Source: HORIBA, INC,
Terahertz Time Domain Spectroscopy

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

Transmission Mode (TM)
- THz pulse Transmitter
- Receiver of the THz pulse

Reflection Mode (RM)
- Receiver of THz pulse
- Transmitter of the THz pulse

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

1. Diversity/Scope

2. Large test time and cost

3. Evolution and trends

4. Complete reliance on subject matter experts (SMEs)

5. Destructive

Source: eenewsanalog.com
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

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

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.

<table>
<thead>
<tr>
<th>Minimum temperature $T_A({}^\circ C)$</th>
<th>Minimum time (h)</th>
<th>Test condition$^3$</th>
<th>Minimum reburn-in time (h)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Class level S$^1$</td>
<td>Class level B$^2$</td>
<td>Class level S hybrids (Class K)</td>
</tr>
<tr>
<td>100</td>
<td>—</td>
<td>352</td>
<td>700</td>
</tr>
<tr>
<td>105</td>
<td>—</td>
<td>300</td>
<td>600</td>
</tr>
<tr>
<td>110</td>
<td>—</td>
<td>260</td>
<td>520</td>
</tr>
<tr>
<td>115</td>
<td>—</td>
<td>220</td>
<td>440</td>
</tr>
<tr>
<td>120</td>
<td>—</td>
<td>190</td>
<td>380</td>
</tr>
<tr>
<td>125</td>
<td>240</td>
<td>160</td>
<td>320</td>
</tr>
<tr>
<td>130</td>
<td>208</td>
<td>138</td>
<td>—</td>
</tr>
<tr>
<td>135</td>
<td>180</td>
<td>120</td>
<td>—</td>
</tr>
<tr>
<td>140</td>
<td>160</td>
<td>105</td>
<td>—</td>
</tr>
<tr>
<td>145</td>
<td>140</td>
<td>92</td>
<td>—</td>
</tr>
<tr>
<td>150</td>
<td>120</td>
<td>80</td>
<td>—</td>
</tr>
<tr>
<td>175</td>
<td>—</td>
<td>48</td>
<td>—</td>
</tr>
<tr>
<td>200</td>
<td>—</td>
<td>28</td>
<td>—</td>
</tr>
<tr>
<td>225</td>
<td>—</td>
<td>16</td>
<td>—</td>
</tr>
<tr>
<td>250</td>
<td>—</td>
<td>12</td>
<td>—</td>
</tr>
</tbody>
</table>

$^1$ 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]

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

Source: Department of Defense, Test Method Standard: Microcircuits
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.

Early Failure Rate (EFR) Data Analysis
- Statistical approach (SVM) to detect recycled ICs.
- Training a one-class classifier using only brand new devices.

Degradation of a critical path

Path Delay Distribution

PCA results: 3 Months

Source: Zhang et al, DFT 2012.

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

Source: Huang et al, DFT 2012.
Section IV: Advanced / Automated Physical Inspection
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

**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
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
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.
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.
1. Depending on the region of chip in question, $1/10^{th}$ 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)
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.
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.

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.
• 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.
“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.
A technique called LBP, or Local Binary Patterns, was used to analyze and classify the texture of regions.
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]<sup>T</sup>
- **E5 (Edge)** = [-1 -2 0 2 1]<sup>T</sup>
- **S5 (Spot)** = [-1 0 2 0 -1]<sup>T</sup>
- **R5 (Ripple)** = [1 -4 6 -4 1]<sup>T</sup>

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

\[
\begin{align*}
(L5E5^T + E5L5^T) & \quad (L5S5^T + S5L5^T) & \quad (L5R5^T + R5L5^T) \\
(E5S5^T + S5E5^T) & \quad (E5E5^T) & \quad (E5R5^T + R5E5^T) \\
(S5R5^T + R5S5^T) & \quad (S5S5^T) & \quad (R5R5^T)
\end{align*}
\]
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.
A two-step methodology combining texture comparison and indent comparison helps to improve the detection accuracy, than only texture based detection [Ghosh and Chakraborty, IEEE TII, 2018].

Unsupervised clustering techniques (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
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 classifier, 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 classifier, four-fold cross-validation was implemented by dividing the data was divided into 75% portion for training and 25% for validation.
  - For the CNN classifier, 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 classifier 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.
• 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

<table>
<thead>
<tr>
<th>Transistors, Diodes, and Passive Parts</th>
<th>Digital &amp; Small</th>
<th>Digital &amp; Large</th>
</tr>
</thead>
<tbody>
<tr>
<td>Programmable Logic ICs</td>
<td>SHIELD, ECID*</td>
<td>SHIELD, DNA, NR</td>
</tr>
<tr>
<td>Memory ICs</td>
<td>SHIELD, SST*</td>
<td>HM*, SST*</td>
</tr>
<tr>
<td>Microprocessor ICs</td>
<td>CDIR*</td>
<td>SHIELD, SST*</td>
</tr>
<tr>
<td>Analog &amp; Mixed Signal ICs</td>
<td>SHIELD, DNA, NR</td>
<td>PUF*, HM*, SST*, NR, DNA</td>
</tr>
</tbody>
</table>

* 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

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

---

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

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

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

- 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

Source: Koushanfar, Springer 2012
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)

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

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

Source: Contreras et al, DFT, 2013
CSST Flow

Test all die and collect responses

ECID and Encrypted TRN's

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

ECID's (Pass)

$R_{IP}$ (avoids collusion)

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

Send FKEY (unique to each chip)

Generate FKEY for ECID (Pass)

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
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
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

**Exploited Characteristics**

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

Source: Alam et al., ITC 2016
Initial Approach (One LUT Path per RO)

**Observation:** Amount of degradation decreases with use

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

Source: Dogan et al., DFT 2014
LUT ‘Types’ Based on Usage

3 bit Adder: \( F = I0 \oplus I1 \oplus I2 \)

(1) Partially Used LUT

Carry out of 4 bit Adder: \( C = ((I0 \times I2) + (I0 \times I3) + (I1 \times I3) + (I2 \times I3) + (I0 \times I1)) \)

(2) Fully Used LUT

Source: Alam et al., ITC 2016
(3) Unused LUT

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


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.

- **Place the XNOR-XOR based Ring Oscillators**
- **Construct Frequency Array**
- **Find the \( \{2, 3, 4, \ldots, K\} \) set of clusters using**
  - Squared Euclidean distance
  - k-means ++ algorithm
  - Local and Global minima avoidance.
- **Calculate the average silhouette value of \( \{2, 3, 4, \ldots, K\} \) clusters set**

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

D. Forte, R.S. Chakraborty
Counterfeit Integrated Circuits: Threats, Detection, and Avoidance

All Rights Reserved
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

- Cells favoring 0 or 1 at startup → ideal for PUF
- Cells that are random at startup → ideal for TRNG
**Neighborhood-based Bit Selection**

- Denotes “stable” bit

<table>
<thead>
<tr>
<th>Cell</th>
<th>Cell</th>
<th>Cell</th>
<th>Cell</th>
<th>Cell</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

E.g.) Window of size 2

<table>
<thead>
<tr>
<th>Cell</th>
<th>Cell</th>
<th>Cell</th>
<th>Cell</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

E.g.) Window of size 4

- 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

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

**Enrollment Phase**

- New SRAM in room/high temperature → Based on Gap and ID, calculate Threshold → ID and Threshold
- Based on Gap, select ASB locations (ID)

**Counterfeit Test Phase**

- SRAM under test in room temperature → Generate Score
- Generate Score → Score > Threshold
  - Yes: Aged
  - No: Fresh

---

**ASBs**: Ageing-Sensitive SRAM Bits

**ID**: ASB locations.

**Important parameters**

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

**Counterfeit test**

- **Score**: a value generated by SRAM under test.

---

Source: Guo et al., HOST 2016

---

D. Forte, R.S. Chakraborty
Counterfeit Integrated Circuits: Threats, Detection, and Avoidance

All Rights Reserved
Area 2: Good performance with respect to accuracy

<table>
<thead>
<tr>
<th>SRAM #</th>
<th>EER</th>
<th>FAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.01</td>
<td>0.00</td>
</tr>
<tr>
<td>2</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>3</td>
<td>0.03</td>
<td>0.00</td>
</tr>
<tr>
<td>4</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

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

Floating Gate Transistors

- Control gate
- Floating gate
- Source
- Drain
- Substrate

- Charge
- In chip controller

Partial programing
- Programming scheduling
- Process variations
- Aging effects

Induce FG failures
- Failure locations
- Insensitive to noise

Wang et al., IEEE S&P 2012
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

100% recycled Flash detection after 5% usage

 Degradation Rate Method

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

![Diagram of PUF (ID) Generation in Flash]

- **Enrollment**
  - 256-bit ID
  - 4,000 P/E cycles

- **Verification**
  - 12,000 P/E cycles
  - 1,000 256-bit IDs

![Histogram of Hamming distance rate with Intra Chip and Inter Chip]
Section VII.A: IP Encryption and IEEE P1735 Standard
ASIC Design Costs (2008)

  - 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

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

Assumption: EDA tool vendor is trusted

Source: Chhotaray et al, CCS, 2017
**IP Encryption Example**

Source: Chhotaray et al, CCS, 2017

**Digital Envelope**

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

Key Block $\rightarrow$ Session key

Data Block $\rightarrow$ Encrypted RTL code

---

D. Forte, R.S. Chakraborty  
Counterfeit Integrated Circuits: Threats, Detection, and Avoidance  
All Rights Reserved
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
   → **Syntax oracle attack (SOA)**
   → **Hardware Trojan insertion and other modifications to IP**

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

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

Initialization Vector (IV)

Key \rightarrow AES Encryption

\[ \cdots \]

Ciphertext

CBC Mode Decryption

Key \rightarrow AES Decryption

\[ \cdots \]

Plaintext
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

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>w/out padding</td>
<td>‘A’</td>
<td>‘E’</td>
<td>‘I’</td>
<td>‘O’</td>
<td>‘U’</td>
<td>‘R’</td>
<td>‘S’</td>
<td></td>
</tr>
<tr>
<td>w/ padding</td>
<td>‘A’</td>
<td>‘E’</td>
<td>‘I’</td>
<td>‘O’</td>
<td>‘U’</td>
<td>‘R’</td>
<td>‘S’</td>
<td>0x01</td>
</tr>
<tr>
<td>w/out padding</td>
<td>‘A’</td>
<td>‘B’</td>
<td>‘C’</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>w/ padding</td>
<td>‘A’</td>
<td>‘B’</td>
<td>‘C’</td>
<td>0x05</td>
<td>0x05</td>
<td>0x05</td>
<td>0x05</td>
<td>0x05</td>
</tr>
</tbody>
</table>

• 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
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).

$$x' = x \oplus g \oplus 0x01$$

Garbage output

$p \neq x \oplus g \rightarrow$
Padding error: $x' \oplus p \neq 0x01$
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

$$x' = x \oplus g \oplus 0x01$$

Garbage output

$p = x \oplus g \rightarrow$

Valid padding: $x' \oplus p = 0x01$
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
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
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 $128 \times N$

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

Source: Chhotaray et al, CCS, 2017
All Rights Reserved
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
Main components

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

- 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

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
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

- 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)

Source: Guin et al, TODAES 2016
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

Source: Guin et al, TODAES 2016
**CUK Exchange Protocol**

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

---

**Source:** Guin et al, TODAES 2016

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
Types of AMS Counterfeits

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

Long life cycle

- Same setup for attackers
- Long term counterfeiting

Single function & small-die

- Less complex design
- Prone to reverse engineering

Market share

- Large market share
- More profit in counterfeiting

Old process technology node

- Low cost fab
- Easy pickings for cloning

Profit margin

- Lower R&D and setup cost
- High demand leads to huge profit
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.

<table>
<thead>
<tr>
<th>The Bad</th>
<th>The Good</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low pin count</td>
<td>PUF, CDIR, etc. access limited</td>
</tr>
<tr>
<td>Lesser process variations</td>
<td>PUF quality impacted?</td>
</tr>
<tr>
<td>Lack of combinational/sequential logic</td>
<td>No crypto for remote communication with chip; obfuscation and locking unsuitable</td>
</tr>
<tr>
<td>Limited test infrastructure</td>
<td>Internal access limits counterfeit detection</td>
</tr>
</tbody>
</table>
Analogue Metering

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

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

Critical Infrastructures

- Military
- Financial
- Civil
- Medical
**Upgrade/Dowgrade Framework**

**System Integration**

- **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.

**Die Integration**

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

Reverse Engineering
- PCB Level
- Chip Level
- Software / Firmware Level

System / Component Profiling
- Reliability
- Performance
- Security

Mapping
- Legacy Spec
- Next-Gen Spec

Validation & Verification

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

<table>
<thead>
<tr>
<th>Discrete</th>
<th>SoCs, uPs, etc.</th>
<th>Memories</th>
<th>FPGAs</th>
<th>AMS</th>
<th>PCB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electrical Tests</td>
<td>Electrical Tests</td>
<td>Electrical Tests</td>
<td>Electrical Tests</td>
<td>Electrical Tests</td>
<td></td>
</tr>
</tbody>
</table>

- 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**

<table>
<thead>
<tr>
<th>Discrete</th>
<th>F-CDIR</th>
<th>PUF</th>
<th>SoCs, uPs, etc.</th>
<th>CDIR</th>
<th>ECID, PUF</th>
<th>FORTIS, HM, SST</th>
<th>SST</th>
<th>FORTIS, HM, SST, camo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memories</td>
<td>CDIR</td>
<td>ECID, PUF</td>
<td>FORTIS, HM, SST</td>
<td>SST</td>
<td>FORTIS, HM, SST, camo</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FPGAs</td>
<td>CDIR</td>
<td>ECID, PUF</td>
<td>FORTIS, HM, SST</td>
<td>SST</td>
<td>FORTIS, HM, SST, camo</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AMS</td>
<td>F-CDIR</td>
<td>ECID? PUF</td>
<td>HM?</td>
<td>Obfuscation? PUF?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCB</td>
<td>Recycled</td>
<td>Remarked</td>
<td>Overproduced</td>
<td>Out-of-Spec/Defective</td>
<td>Cloned</td>
<td>Tampered</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 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