Covert Gates: Protecting Integrated Circuits with Undetectable Camouflaging

Bicky Shakya, Haoting Shen, Mark Tehranipoor and Domenic Forte
Rise of Automated Reverse Engineering

- Chip
- De-packaging
- De-layering & Imaging
- Layout Generation
- Netlist Extraction

- Chemicals & Abrasion
- Polishing & Delayering

- Evaluate its performance and functionality
- See if it infringes your patents
- See how competitor product matches up

- Integrate the IP into an attacker’s design
- Clone the design
- Find and exploit vulnerabilities in the design

Source: scienceasart.org
Source: micronetsol.net, texplained.com
What is IC Camouflaging?

Main Goal: Protect IP from Reverse Engineering

Stakeholders: Commercial Semiconductor Design Houses and Fabless Vendors, IP Providers (even Foundries), and Government (esp. Defense)
Existing Camouflaging Techniques

Camouflaging (Camo) Gate: hide the real gate’s function

Camouflaging Gate Design Examples

Dummy Contact [Rajendran et al, CCS 2013]

Threshold-Voltage Modification [Erbagci et al., HOST 2016]

Drawbacks

- 4-5x Larger Power and Area
- Different Logic Style
- > 2x Area, 1.5x Delay, and 10% Power
**Scope and Adversarial Model**

**Assumption #1 (Defense):** Foundry is trusted
- Plays an active role in protecting the IP
- May even provide library of camo cell technologies
- Does not leak GDSII, mask sets, etc.

**Assumption #2 (Attack):** The following are available to the attacker

- A *Camouflaged* Netlist (obtained by RE)
- A Functional Chip (i.e., Oracle)
- Scan Chain Access

In-field reverse engineering
Attacks on Prior IC Camouflaging Approaches

**Overhead Cost → Limited No. of Camouflaging → Attack Vector**

**Automatic Test Pattern Generation (ATPG)**

- **Steps:**
  1. Build equivalent circuit encoding (camo → logic locked)
  2. Apply input patterns at PI, scan-in to sensitize camo gate inputs
  3. Use test response to resolve gate functionality

**Satisfiability-based (SAT) Attack**

- **Steps:**
  1. Build equivalent circuit encoding
  2. Observe the satisfiability using oracle
  3. Rule out incorrect assignments

[Massad et al., NDSS 2015, Subramanyan et al., HOST 2015]

[Rajendran et al., DAC 2012, Vontela et al., ISQED 2017]
Proposed Approach: ‘Covert’ Camo Gate

Requirements

- Every camouflaged gate should look like any other gate in a standard cell library
  - All gates become suspect!
  - Expected to drastically increase invasive and non-invasive attack complexity

Covert Gate

- Expand \( n \) input gates into \( n + i \) input gates (where \( i \) is # of dummy inputs)
  + Much lower leakage/area/delay expected with dummy inputs
  + No change in logic style
**‘Covert’ Gate Schematic Design**

**Regular MOSFET modification**
Switchable transistors → [Always-On] or [Always-Off]
Modification is **INVISIBLE** by SEM

**Complementary structure is necessary:**
1. Enable functional gates
2. Keep the static current leakage low

**Implemented modification: Dummy Inputs**

\[
\begin{align*}
\text{Always-On in the pull-up} & \quad \text{Always-Off in the pull-down} \\
\text{Always-Off in the pull-up} & \quad \text{Always-On in the pull-down}
\end{align*}
\]
Device Structure and Fabrication of Covert Gates

Regular

Always-On

Regular

Always-Off
‘Always on’ Prototype Structure

**Top-views**

- **Regular**
  - 90nm

- **Always on**
  - Shallow doping (always-on channel)

**Cross-sections**

- Regular doping (source/drain)
- Shallow doping (always-on channel)

**Imaging Settings**

<table>
<thead>
<tr>
<th></th>
<th>SE</th>
<th>BSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 keV</td>
<td>15 keV</td>
<td></td>
</tr>
<tr>
<td>10 keV</td>
<td>10 keV</td>
<td></td>
</tr>
<tr>
<td>5 keV</td>
<td>5 keV</td>
<td></td>
</tr>
<tr>
<td>800 eV</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
Imaging Results – Regular vs. Always-On

**PMOS**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Image 1</th>
<th>Image 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMOS, 5 keV, SE</td>
<td>Regular Set 1</td>
<td>Always On Set 1</td>
</tr>
<tr>
<td>PMOS, 5 keV, BSE</td>
<td>Regular Set 1</td>
<td>Always On Set 1</td>
</tr>
<tr>
<td>Gap designed to be 90 nm</td>
<td>Always On</td>
<td>Regular</td>
</tr>
</tbody>
</table>

**NMOS**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Image 1</th>
<th>Image 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>NMOS, 5 keV, BSE</td>
<td>Regular Set 1</td>
<td>Always On Set 1</td>
</tr>
<tr>
<td>Gap designed to be 90 nm</td>
<td>Always On</td>
<td>Regular</td>
</tr>
</tbody>
</table>
Imaging Results – Regular vs. Always-Off

Regular Contacts

SiO₂

Au

Contact

Si wafer

Gate

Dummy Contacts

SiO₂

Au

Dummy Contact

Si wafer

Regular

Real Contacts Row
100 nm  300 nm  500 nm  1 μm  1.5 μm  2 μm

800 eV, SE

Dummy Contacts Row
100 nm  300 nm  500 nm  1 μm  1.5 μm  2 μm

Top View (SEM)
Top: SE
Bottom: BSE

Dummy

Real Contacts Row
100 nm  300 nm  500 nm  1 μm  1.5 μm  2 μm

15 keV, BSE

Dummy Contacts Row
100 nm  300 nm  500 nm  1 μm  1.5 μm  2 μm

Cross-section (Prototype)

Top View (SEM)
Top: SE
Bottom: BSE

SiO₂₂

p wafer

n+
gate

n+
Experimental Setup

- **SAT Attack:** Scenario #3, timeout set at 12 hours
- **Test-based Attack:** Scenario #2
- **Covert Gate Insertion:** Random, but combination feedbacks are not allowed

**Diagram Notes:**
- **Higher Attack Complexity:**
  - Less knowledgeable attacker
  - No information on which gates are camouflaged

- **Lower Attack Complexity:**
  - More knowledgeable attacker
  - Only specific gates (and specific pins) can be camouflaged gates

**Legend:**
- Fan-in cone modification, enabled by dummy inputs
SAT Attack Formulation on Covert Gates

- Correct key chooses correct pins **based on oracle response**
- **Complexity increase** with
  - No. of pins on suspect gates
  - No. of candidate gates → *all gates*
  - Increased conjunctive normal form (CNF) formula size → *Larger search space*
SAT Attack Results

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>Gate / Node Count</th>
<th>Existing Camo</th>
<th>Proposed Camo (Covert)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>$</td>
<td>K</td>
</tr>
<tr>
<td>C1908</td>
<td>880</td>
<td>34</td>
<td>0.55</td>
</tr>
<tr>
<td>C2670</td>
<td>1193</td>
<td>26</td>
<td>0.65</td>
</tr>
<tr>
<td>C3540</td>
<td>1669</td>
<td>28</td>
<td>0.68</td>
</tr>
<tr>
<td>C5315</td>
<td>2307</td>
<td>46</td>
<td>3.58</td>
</tr>
<tr>
<td>C7552</td>
<td>3512</td>
<td>106</td>
<td>4.07</td>
</tr>
<tr>
<td>arbiter</td>
<td>11,839</td>
<td>1182</td>
<td>3815.00</td>
</tr>
<tr>
<td>voter</td>
<td>13,758</td>
<td>1078</td>
<td>Timeout</td>
</tr>
</tbody>
</table>

SAT Attack Complexity

- Increased key size
- SAT attack timeout (12 hrs) → More iterations / More time per iteration
Test-Based Attack Results

Generate a test to check whether pin is dummy or functional.
- **Control**: Assert controlling value on suspect pin (using s-a-0, s-a-1)
- **Observe**: Non-controlling values on other pins and nets to propagate to observe point

Possible Scenarios
- **Detectable**: it can be determined with certainty whether a pin on the gate is dummy or not
- **Undetectable**: the dummy pin has no effect on the output ‘ATPG
- **Untestable**: a test pattern cannot be generated to sensitize and propagate a controlling value on a potentially dummy pin
- **Not Detected**: test pattern to detect the pin could not be generated with tool effort level

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>Gate</th>
<th>Gate Count</th>
<th>Detectable</th>
<th>Undetectable</th>
<th>ATPG Untestable</th>
<th>Not Detected</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>#</td>
<td>%</td>
<td>#</td>
<td>%</td>
</tr>
<tr>
<td>b18</td>
<td>NOR2X</td>
<td>2390</td>
<td>10</td>
<td>0.42</td>
<td>5</td>
<td>0.21</td>
</tr>
<tr>
<td>Primitive Count = 84,632</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NOR3X</td>
<td>270</td>
<td>12</td>
<td>4.44</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>NOR4X</td>
<td>195</td>
<td>17</td>
<td>8.72</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>NAND2X</td>
<td>4194</td>
<td>7</td>
<td>0.17</td>
<td>30</td>
<td>0.72</td>
</tr>
<tr>
<td></td>
<td>NAND3X</td>
<td>2135</td>
<td>8</td>
<td>0.37</td>
<td>19</td>
<td>0.89</td>
</tr>
<tr>
<td></td>
<td>NAND4X</td>
<td>909</td>
<td>38</td>
<td>4.18</td>
<td>0</td>
<td>0.00</td>
</tr>
</tbody>
</table>

Legend
- Attack succeeds
- Attack fails

> 91%
Circuit Overhead and Corruptibility Results

- **Minimal area overhead.** Proposed camo cells are no larger than standard logic gates (AND2X1, NAND2X1 etc.)
- **Power overhead minimal**
- **Delay penalty due to random insertion.** Can avoid critical paths for further optimization
- **High Corruptability.** Even when covert gates are inserted randomly, there are large number of percentage mismatches with original design

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>Area (µm²)</th>
<th>Delay (ns)</th>
<th>Power (µW)</th>
<th>Verification Failure (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Covert</td>
<td>Original</td>
<td>%</td>
<td>Covert</td>
</tr>
<tr>
<td>AES</td>
<td>114,098</td>
<td>113,384</td>
<td>0.63</td>
<td>18.19</td>
</tr>
<tr>
<td>b12</td>
<td>9,725</td>
<td>9,646</td>
<td>0.81</td>
<td>2.98</td>
</tr>
<tr>
<td>b15</td>
<td>53,432</td>
<td>53,134</td>
<td>0.56</td>
<td>26.32</td>
</tr>
<tr>
<td>b17</td>
<td>171,193</td>
<td>170,264</td>
<td>0.54</td>
<td>32.47</td>
</tr>
<tr>
<td>s35932</td>
<td>111,402</td>
<td>111,088</td>
<td>0.28</td>
<td>14.13</td>
</tr>
<tr>
<td>s38417</td>
<td>107,803</td>
<td>107,349</td>
<td>0.42</td>
<td>20.84</td>
</tr>
<tr>
<td>s38584</td>
<td>87,647</td>
<td>87,229</td>
<td>0.48</td>
<td>15.38</td>
</tr>
</tbody>
</table>
Acknowledgements

We are grateful for the sponsors of this project:

Thank you to the partners and sponsors of UF/FICS SCAN Lab:
Conclusion and Future Work

Covert gates

- Indistinguishable from regular gates (i.e., imaging resistant)
- Very strong deterrents against oracle-based and probing-based reverse engineering
- Inexpensive to fabricate
- Lower overhead than existing camo gates

Future Work

- Formal proofs of security against oracle attacks
- Investigate oracle-less attacks (e.g., structural) against covert gate circuits
- Explore covert gate insertion strategies w/ security and overhead in mind
- Fabricate and characterize real covert gate devices
- Image using He-Ne ion microscopes
Conclusion and Future Work

Covert gates
• Indistinguishable from regular gates (i.e., imaging resistant)
• Very strong deterrents against oracle-based and probing-based reverse engineering
• Inexpensive to fabricate
• Lower overhead than existing camo gates

Future Work
• Formal proofs of security against oracle attacks
• Investigate oracle-less attacks (e.g., structural) against covert gate circuits
• Explore covert gate insertion strategies w/ security and overhead in mind
• Fabricate and characterize real covert gate devices
• Image using He-Ne ion microscopes
## Covert Gate Distribution for SAT Evaluation

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>Total % Covert</th>
<th>2 input</th>
<th>3 input</th>
<th>4 input</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>AND/NAND</td>
<td>OR/NOR</td>
<td>AND/NAND</td>
</tr>
<tr>
<td>C1908</td>
<td>45%</td>
<td>43%</td>
<td>0%</td>
<td>1%</td>
</tr>
<tr>
<td>C2670</td>
<td>56%</td>
<td>38%</td>
<td>5%</td>
<td>9%</td>
</tr>
<tr>
<td>C3540</td>
<td>56%</td>
<td>41%</td>
<td>4%</td>
<td>6%</td>
</tr>
<tr>
<td>C5315</td>
<td>60%</td>
<td>34%</td>
<td>5%</td>
<td>16%</td>
</tr>
<tr>
<td>C7552</td>
<td>58%</td>
<td>44%</td>
<td>6%</td>
<td>4%</td>
</tr>
<tr>
<td></td>
<td>100%</td>
<td>100%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>100%</td>
<td>100%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>
Covert Gate Circuit Model

- **Always-on FET** emulated by depletion mode device where channel is ‘pre-formed’

- **Always-off FET** emulated by SiO2 insulator in gate and source contacts

---

**Overhead Cost (SPICE Simulations)**

<table>
<thead>
<tr>
<th>Dummy-based Camouflaging Gates</th>
<th>Proposed Covert Gates (Compared to INVX1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area</td>
<td>Delay</td>
</tr>
<tr>
<td>4 X</td>
<td>1.6 X</td>
</tr>
<tr>
<td>4 X</td>
<td>1.1 X</td>
</tr>
</tbody>
</table>
Effective Conduction Volumes (Proposed)
Reversing Stealthy Dopant-level Trojans

Sugawara et al, CHES 2014

- **Passive Voltage Contrast (PVC)** is a measurement principle used by SEM/FIB to measure surface voltage of a sample.
- Dopant configurations used by dopant-level Trojans can be distinguished with PVC even when a chip is measured at power-off state!
Etching

Cross-section

Top View
Comparison to Other Camouflaging Techniques

<table>
<thead>
<tr>
<th>Feature</th>
<th>Regular Camouflaging</th>
<th>Covert Gates</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dummy Contact</td>
<td>Threshold Voltage</td>
</tr>
<tr>
<td>SAT resistant at low overhead</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Test attack resistant</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Low overhead</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Configurable after fabrication</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Imaging resistant</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Undetectable during netlist extraction</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>
SEM Images: NMOS, 15 keV, SE and BSE
SEM Images: NMOS, 10 keV, SE and BSE
SEM Images: NMOS, 5 keV, SE and BSE

NMOS, 5 keV, SE

1.5 um

Regular Set 1

Always On Set 1

Always On Set 2

Regular Set 2

50 um

NMOS, 5 keV, BSE

Regular Set 1

Always On Set 1

Always On Set 2

Regular Set 2

50 um
SEM Images: NMOS, 800 eV, SE and BSE

BSE mode is not available with 800eV
SEM Images: PMOS, 15 keV, SE and BSE
SEM Images: PMOS, 10 keV, SE and BSE
SEM Images: PMOS, 5 keV, SE and BSE
SEM Images: PMOS, 800 eV, SE and BSE

BSE mode is not available with 800eV
A globalized semiconductor supply chain leads to the possibility of IP exposure and compromise at almost every stage. Consequences range from lost revenue to design tampering. IP is the backbone of every chip and needs active protection mechanisms at various abstraction in the supply chain, where IP has always been a focus of protection. }

From the SEMI President and CEO
Innovation is at Risk: Losses of up to $4 Billion Annually due to IP Infringement

Protection of intellectual property (IP) rights is an important area of concern for the semiconductor manufacturing industry. In a competitive global business environment, IP protection is essential to the survival of equipment and materials suppliers, enabling them to invest the significant R&D funds needed to sustain technological advancement of the semiconductor industry.

In recent years, suppliers have been increasingly funding a larger portion of the escalating R&D costs needed for the continued success of the semiconductor device industry. These challenging conditions pose a serious threat to the IP supply chain, where IP has always been a primary focus of protection, generation of equipment and materials, and the technology curve.

In recent years, the importance of IP protection has increased, and companies are taking active measures to safeguard their intellectual property. The following examples illustrate the challenges and solutions being employed to combat IP infringement:

1. **Reverse Engineering**:
   - Chipworks, a company known for reverse-engineering semiconductor designs, recently revealed a 14nm Broadwell chip design that was reverse-engineered from public information. The detailed design information includes the various layers of abstraction involved in the chip design, ranging from the architectural to the physical layers. This information is invaluable for understanding the design process and for developing new technologies.

2. **IP Misuse, Theft**:
   - Engineers at a well-known electronics company, who had access to confidential IP data, were accused of stealing trade secrets. The stolen information included detailed schematics and intellectual property that could have been used to develop rival products. The theft of this information posed a significant threat to the company's competitive advantage.

These examples highlight the importance of IP protection in the semiconductor industry. Companies are investing in advanced technologies and robust security measures to ensure the integrity of their intellectual property. The semiconductor supply chain is continually evolving, and so must the strategies for protecting IP.
SAT Attack Formulation on Covert Gates

- Correct key chooses correct pin permutation network

- Complexity increase with:
  - No. of pins on suspect gates
  - No. of candidate gates → all gates
  - Increased conjunctive normal form (CNF) formula size → Larger search space

Non-controlling value

\[ F \]

\[ K_1 \]

\[ K_2 \]

\[ N \]

\[ K_N \]
Device Structure and Fabrication of Covert Gates

Regular

Always-On

Regular

Always-Off

p wafer

n+

gate

p wafer

n+

gate

p wafer

n+

gate

p wafer

n+

gate

p wafer

n+

gate

SiO$_2$

n+

gate

p wafer

n+

gate

p wafer

n+

gate

SiO$_2$

M

M

SiO$_2$

n+

gate

p wafer

n+

gate

SiO$_2$

M

M

SiO$_2$

n+

gate

p wafer

n+

gate

SiO$_2$