Anti-Reverse Engineering using Transient Electronics

Lei Wang and John Chandy

University of Connecticut
Hardware Attacks Based on Reverse Engineering

### Chip-level Attacks

- **Trojan Insertion**
  RE discover the original design (RTL-level or gate-level) of the targeted IC for Trojan insertion

- **Patent Infringement**
  RE makes patent infringement hard to be identified.

- **Micro-probing**
  Eavesdropping on sensitive data

- **Backdoor Insertion**
  Backdoors make cyberattacks much easier.

### PCB-level Attacks

- **Trojan insertion**
  Trojan Insertion requires minimal design knowledge

- **Brutal Copying**
  Brutal copying benefits competitors because of short leading time and low cost

- **Degradation**
  Attackers modify the physical size of metal traces to trigger durability issue or performance degradation
Reverse Engineering at Chip Level

1. Decapsulating/Depackaging

- Encapsulation typically used to protect circuitry from moisture, dust, mold, or corrosion
- Hot air gun to soften epoxy
- Chemicals
- Dremel tool and wooden skewer as a drill bit

2. Delayering/Deprocessing

- The delayering process is a combination of wet chemical, mechanical and plasma processes to prepare for imaging
Reverse Engineering at Chip Level

3. Imaging

- CMOS feature sizes hit the diffraction limit of optical microscopes: Scanning Electron Microscope (SEM) or Focused Ion Beam (FIB)
- SEM images is beneficial for post-process as it allows to distinguish between vias and wires

4. Software-based Post-processing

- Cell Matching: Some standard cells, including their rotated or mirrored version, can be identified.

5. System recovery

- Higher level information extraction (e.g. control units or submodules)
- Gate-level netlist reverse techniques can be applied.
Magnesium displays very good electrical conductivity. The resistivity of Mg (44.7 nΩ·m) is lower than tungsten (56.1 nΩ·m), which has been widely used as the material for vias.

The resistivity of magnesium oxide at room temperature is 1014 Ω·cm, similar to silicon dioxide.

Magnesium can completely oxidize into magnesium oxide in a very short time.

According to the diffraction pattern, X-ray imaging cannot differentiate MgO and Mg easily.
Translucent Electronics for Chip Anti-RE

- Mg is used as the material for some contacts and vias.
- Dummy interconnects are deliberately introduced, which are connected through non-conductive MgO contacts/vias to certain circuit nodes.
- During the delayering process, magnesium will completely oxidize into magnesium oxide.
- In imaging, MgO vias will be identified as Mg vias.
- Mg/MgO material pairs will lead attackers to another routing pattern.

Fabricated SRAM cell

Top view

Cross-section view
Super Connection Nodes

- Adding transformable interconnects forms SCNs and increases the fanout of logic gates.
- The complexity introduced by an SCN can be defined as the number of possible “valid” designs (i.e., obeying the design rule) to fix this SCN.
- In general, for an SCN with n-fanout and m-fanin, the total number of “valid” circuits can be expressed as:

\[ N_m = \sum_{i_1, i_2, \ldots, i_n} C_{m}^{i_{m-i_1}} C_{m-1}^{i_{m-i_1-i_2}} \cdots C_{2}^{i_{m-i_1-i_2-\cdots-i_{n-1} -1}} C_{1}^{i_n} \]
Consideration of Behavioral Information

- Select a subset of all existing nodes for transformable interconnect insertion: low design overhead, maximal effectiveness

- Switching activity: circuit nodes with higher switching activities are more likely to propagate signals as well as faults than those with low switching activities.

- Correlation coefficient: A transformable interconnect will make a faulty connection between two circuit nodes. Ideally, the behavior of these two nodes should be as different as possible

\[ \gamma_{BE} = -0.577, \gamma_{CE} = 0 \]
## Evaluations

- **ITC99 benchmarks with different levels of timing overhead.**
- \( N \) is the number of inserted transformable interconnects, \( \alpha_{\text{min}} \) refers to the minimal value of switching activity, \( \gamma_{\text{max}} \) indicates the correlation coefficient among the selected node pairs.
- A large value of \( N_m \) means more difficult for the attacker to derive the original design.

<table>
<thead>
<tr>
<th>ITC99</th>
<th>gates</th>
<th>0% timing overhead</th>
<th>3% timing overhead</th>
<th>5% timing overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>( N )</td>
<td>( N_m )</td>
<td>( \alpha_{\text{min}} )</td>
<td>( \gamma_{\text{max}} )</td>
</tr>
<tr>
<td>b05</td>
<td>7</td>
<td>141120</td>
<td>0.218</td>
<td>-0.20</td>
</tr>
<tr>
<td>b12</td>
<td>12</td>
<td>1.11e7</td>
<td>0.243</td>
<td>-0.32</td>
</tr>
<tr>
<td>b14</td>
<td>30</td>
<td>3.87e15</td>
<td>0.251</td>
<td>-0.24</td>
</tr>
<tr>
<td>b14_1</td>
<td>6900</td>
<td>6.31e18</td>
<td>0.197</td>
<td>-0.23</td>
</tr>
<tr>
<td>b15</td>
<td>38</td>
<td>5.75e23</td>
<td>0.184</td>
<td>-0.27</td>
</tr>
<tr>
<td>b20</td>
<td>48</td>
<td>7.23e29</td>
<td>0.172</td>
<td>-0.22</td>
</tr>
<tr>
<td>b21</td>
<td>54</td>
<td>1.67e32</td>
<td>0.136</td>
<td>-0.15</td>
</tr>
<tr>
<td>b22</td>
<td>76</td>
<td>5.15e37</td>
<td>0.227</td>
<td>-0.43</td>
</tr>
<tr>
<td>b17</td>
<td>92</td>
<td>1.21e48</td>
<td>0.166</td>
<td>-0.28</td>
</tr>
<tr>
<td>b17_1</td>
<td>96</td>
<td>1.76e56</td>
<td>0.149</td>
<td>-0.12</td>
</tr>
<tr>
<td>b18</td>
<td>265</td>
<td>5.33e116</td>
<td>0.215</td>
<td>-0.30</td>
</tr>
<tr>
<td>b18_1</td>
<td>225</td>
<td>1.62e109</td>
<td>0.185</td>
<td>-0.18</td>
</tr>
<tr>
<td>b19</td>
<td>438</td>
<td>3.90e201</td>
<td>0.203</td>
<td>-0.09</td>
</tr>
<tr>
<td>b20_1</td>
<td>71611</td>
<td>482</td>
<td>1.01e230</td>
<td>-0.04</td>
</tr>
</tbody>
</table>
Conclusions

• Chip design using Mg-MgO based transient electronics for anti-reverse engineering

• Evaluation of the effectiveness, feasibility and performance of Mg as an interconnect material

• Design methods for the placement of dummy MgO wires in an anti-reverse engineering setting

• Simulation results demonstrate the effectiveness of this method with minimal performance overhead and design cost