A Perspective on Security and Trust Requirements for the Future

Dr. Kenneth Plaks

International Symposium on Physical Design

April 14-17, 2019
The importance of electronics
### Commercial

- IP protection and overproduction
- License Enforcement
- Brand identity and dependability

### Military

- Export leakage – ITAR concerns
- Anti Tamper
- Trust – reliability and no malicious insertions
But we place a much higher priority on security

What would physical design look like if we optimized for security, instead of area?
(U) Physical design and security

Side Channels

Digital World

Physical Design

Real World

Sensors
• For this talk, sensors are things that provide data from the real world to the digital world
  • Military uses sensors to determine where a chip has been
  • Military uses sensors as a root of trust
• We will use the DARPA SHIELD project as an example

Image courtesy of Northrop Grumman

Image courtesy of SRI International
Sensor Example: DARPA SHIELD

Key SHIELD Specifications
- Unique Key Storage
- Full 256-bit AES encryption engine
- Unpowered, passive intrusion sensors
- RF power and communication
- Transfer fragility
- 100µm x 100µm
- 50 µW Total Power
- Operating temp < 120°C
- Cost < $0.01 per dielet

Asymmetric Security
- Non-resettable, “always on” intrusion sensors on dielet
- On-board encryption symmetric key that cannot be “coaxed” from dielet
- ID and Key are unique to the individual host IC (not just the part number)
- Interrogation history (date, time, location) stored on secure server
- Built-in fragility structures kill dielet if removal from host is attempted

SHIELD makes counterfeiting too expensive and too hard to do.
Mini-x-ray test fixture in Draper’s Radiation Effects Lab

Stock photos of anechoic chamber, antenna & probe. RF testing was carried out in a secure lab at Draper

Sensor Radiation Sensitivity

Voltage (V) vs. Dose in KRad(Si) graph

Distribution Statement A: Approved for Public Release, Distribution Unlimited
Physical Vulnerabilities of PUFs

The 1st silicon iteration of a DoD PUF failed due to its output voltages being severely skewed in the negative direction (toward 0V)

The root cause of the voltage skew was the layout proximity effect which is a dominant effect in nanoscale devices

The PUF voltages should have been uniformly distributed; however, testing revealed that most of the voltages were skewed negatively toward 0V.
Side channels

- For this talk, side channels are ways of getting data from the digital world to the real world
  - Not talking about SPECTER and MELTDOWN
  - Military uses side channels to find malicious circuits
- How can we interrogate a circuit for malice, when we don’t trust the circuit in the first place?
- What aspects of physical design could enhance security?
The trojan challenge in three charts

Moore’s law makes SOC’s possible

Technical Observation

But we have lost herd immunity
Moore’s law also makes defense even harder
One possible approach: physical timing side channels

- Trojan impact on timing should be observable even without activating the trojan
- But voltage variation makes that hard to measure

Solution to Complications:

- **Voltage Noise**

- **Process Drift**

Avesta Sasan, GMU


https://dl.acm.org/citation.cfm?id=3287683
Spice Verification: the improved accuracy of AVATAR (IR-ATA) in capturing the timing impact of Voltage drop (STA versus Spice)

STA Improvement: Impact of using AVATAR(IR-ATA) for reporting the timing slack:
- The released slack could be used for PPA improvement.

The timing slacks in two nearly timing closed design (DES3 and AES) using conventional margin based and AVATAR flow for generation of GTM.
**Power reduction:** The released slack (from using AVATAR for voltage drop and voltage noise modeling) is used for ECOs targeting the reduction of leakage and dynamic power.

- Reduces Dynamic power
- Reduces Leakage power
- Reduces area

**Performance boost:** The released slack (from using AVATAR for voltage drop and voltage noise modeling) in critical timing paths, allow the physical designer to shorten the clock cycle time, leading to a higher performance design.

- Increases max frequency

---

**PPA Improvement**

Summary of power & area improvement in the investigated benchmarks when STA is updated with IR-ATA flow, followed by incremental application of power and timing ECOs.

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>Percentage Reduction</th>
<th>Fixed Timing Violations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dynamic P</td>
<td>Leakage P</td>
</tr>
<tr>
<td>DES3</td>
<td>1.9</td>
<td>13</td>
</tr>
<tr>
<td>AES</td>
<td>2.3</td>
<td>11</td>
</tr>
<tr>
<td>b19</td>
<td>1.6</td>
<td>19</td>
</tr>
<tr>
<td>MSP430</td>
<td>2.4</td>
<td>18</td>
</tr>
<tr>
<td>ETHERNET</td>
<td>2.3</td>
<td>13</td>
</tr>
<tr>
<td>s38417</td>
<td>1.9</td>
<td>21</td>
</tr>
</tbody>
</table>

Summary of improvement in the performance (max frequency) of investigated benchmark when STA is updated with IR-ATA and increase in total available slack in top 10K timing paths (to be used for dynamic power, leakage & area recovery).

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>Total Available Slack (ns) Before</th>
<th>Total Available Slack (ns) After</th>
<th>Max Freq (GHz) Before</th>
<th>Max Freq (GHz) After</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES3</td>
<td>8351.26</td>
<td>8859.78</td>
<td>0.72</td>
<td>0.76</td>
</tr>
<tr>
<td>AES</td>
<td>3033.56</td>
<td>33045.42</td>
<td>1.05</td>
<td>1.09</td>
</tr>
<tr>
<td>b19</td>
<td>1608.30</td>
<td>1720.31</td>
<td>0.46</td>
<td>0.48</td>
</tr>
<tr>
<td>MSP430</td>
<td>842.51</td>
<td>903.09</td>
<td>0.33</td>
<td>0.34</td>
</tr>
<tr>
<td>ETHERNET</td>
<td>8347.31</td>
<td>8905.58</td>
<td>0.53</td>
<td>0.54</td>
</tr>
<tr>
<td>s38417</td>
<td>499.07</td>
<td>576.16</td>
<td>1.07</td>
<td>1.12</td>
</tr>
</tbody>
</table>

Avesta Sasan, GMU
The new voltage variation aware timing model (GTM) along with NN process watch dog can significantly improve the chances of Trojan detection without having access to a Golden IC.

**Design and test Flow**

**Trojan Detection**

**AES128**

**Ethernet**

**S38417**

Avesta Sasan, GMU
Security aware physical design

Routing VIA: Adapt via size to help enhance power estimation accuracy

- Adaptive approach VIA: Lower resistance. Larger routing resources.
- Smaller VIA: Highest resistance. Largest routing resources.
- Large VIA: Lowest resistance. Lowest routing resources.

- Upsize critical VIAs
- Adds less routing violations

Decap: Insert decaps to help stabilize power estimate


- Leakage reduction
- Lower space overhead

Summary of change in Vmax, number of routing violations, and percentage of upsized via stacks when using IR-ATA enabled via stack re-sizing in Algorithm 2.

<table>
<thead>
<tr>
<th>Design (DES)</th>
<th>Vmax</th>
<th>Routing Violations</th>
<th>% via upsized</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1× 2) Vias</td>
<td>0.895</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>IR-ATA-Adaptive Via</td>
<td>0.909</td>
<td>9</td>
<td>14.34</td>
</tr>
<tr>
<td>(4× 2) Vias</td>
<td>0.910</td>
<td>2651</td>
<td>100</td>
</tr>
</tbody>
</table>

IR-ATA enabled Decap insertion uses only half of empty spaces, but reaches similar $V_{max}$ to the design fully packed by decaps, resulting in 2.6% reduction in leakage.

<table>
<thead>
<tr>
<th>Design (DES)</th>
<th>$V_{max}$</th>
<th>Leakage Reduction</th>
<th>% empty space used</th>
</tr>
</thead>
<tbody>
<tr>
<td>With Decap</td>
<td>0.912</td>
<td>0</td>
<td>98.84</td>
</tr>
<tr>
<td>Proposed ECO</td>
<td>0.911</td>
<td>2.15%</td>
<td>42.53</td>
</tr>
<tr>
<td>No Decap</td>
<td>0.897</td>
<td>3.85%</td>
<td>0</td>
</tr>
</tbody>
</table>
Conclusion

- Physical design is where the digital becomes real
- There are several opportunities to enhance security
  - Or inadvertently break it...
- By adding security considerations to physical design offers the opportunity to make better chips, with lower security risk

To make security-aware physical design a reality