rFAS
-
reconfigurable FPGA Accelerator Sandboxing

Dirk Koch, Tuan La, Khoa Pham
{dirk.koch,tuan.la,khoa.pham@manchester.ac.uk)
Department of Computer Science
The University of Manchester
FPGAs have a huge surface of attack!

- Remote DPA attacks
- Destroy or age FPGA hardware through corrupted bitstream (we have shown that!)
- Power hammering attacks
## Study on Ring-Oscillators

<table>
<thead>
<tr>
<th>Schematics</th>
<th>Measured Frequency</th>
<th>Power</th>
<th>WPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ø</td>
<td>Ø</td>
<td>2.94W</td>
<td>Ø</td>
</tr>
<tr>
<td><img src="image" alt="LUT6 Diagram" /></td>
<td>5882MHz</td>
<td>7.32W (+4.38W)</td>
<td>26.63</td>
</tr>
<tr>
<td><img src="image" alt="LUT6 Diagram" /></td>
<td>3937 MHz</td>
<td>6.84W (+3.90W)</td>
<td>23.69</td>
</tr>
</tbody>
</table>
# Study on Ring-Oscillators

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Frequency</th>
<th>Power Consumption</th>
<th>Power Increase</th>
</tr>
</thead>
<tbody>
<tr>
<td>1's1 15 13 12 11 10 14</td>
<td>O5: 1235MHz, O6: 2439MHz</td>
<td>8.04W (+5.10W)</td>
<td>31.00</td>
</tr>
<tr>
<td></td>
<td>1779MHz</td>
<td>9.61W (+6.66W)</td>
<td>40.54</td>
</tr>
<tr>
<td>CARRY8</td>
<td>1681MHz</td>
<td>4.04W (+1.10W)</td>
<td>1.67</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>----------------</td>
<td>------</td>
</tr>
<tr>
<td>MUXCY</td>
<td>1109MHz</td>
<td>5.14W (+2.19W)</td>
<td>1.67</td>
</tr>
<tr>
<td>DSP48E2</td>
<td>585MHz</td>
<td>4.53W (+1.59W)</td>
<td>0.27</td>
</tr>
</tbody>
</table>

**Diagram:**
- **CARRY8** block diagram with inputs and outputs.
- **MUXCY** block diagram showing carry selection.
- **DSP48E2** block diagram with inputs and outputs.
# Study on Ring-Oscillators

<table>
<thead>
<tr>
<th>Diagram</th>
<th>Frequency</th>
<th>Power</th>
<th>Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Diagram" /></td>
<td>1706MHz</td>
<td>5.14W (+2.19W)</td>
<td>13.35</td>
</tr>
<tr>
<td><img src="image2.png" alt="Diagram" /></td>
<td>555MHz</td>
<td>5.26W (+2.32W)</td>
<td>7.05</td>
</tr>
<tr>
<td><img src="image3.png" alt="Diagram" /></td>
<td>481MHz</td>
<td>8.05W (+5.10W)</td>
<td>10.35</td>
</tr>
</tbody>
</table>
Study on Ring-Oscillators

Experiment: 2K LUTs on a Ultra96 Board (Xilinx Zynq UltraScale+)

- The fastest oscillators do not necessarily burn most power
- Fast oscillators are better for power analysis attacks
Study on Ring-Oscillators

*Recommended core voltage

**Board crashes at this value

LUT Utilization for ROs (%) 5.2%**
Study on Ring-Oscillators

We carried out first experiments on an Alveo U200* datacenter FPGA → 10% LUTs draw 350W !!!
(* same specification as used in Amazon F1)

- x KW Power-hammering potential!
- Many of our circuits are not spotted by the vendor tools!
  (Design Rule Checks (DRCs) & power analyzer tool)
- We tested power-hammering attacks on Amazon F1 instances:
  → can be deployed!
- Oscillators allow power analysis attacks
  (finger printing (PUFs), temperature, attack triggers, ...
FPGADefender Virus Scanning for FPGAs

- Detects probably any kind of self-oscillating circuits
- Scans bitstream encoding (short circuits), high fan-out nets, wire tapping, module bounding boxes (all at bitstream level)
- more to come …
Major outcome:

FPGADefender

People:

- Tuan Minh La  {tuan.la@postgrad.manchester.ac.uk}
- Khoa Dang Pham  {khoa.pham@manchester.ac.uk}
- Kaspar Matas  {kaspar.matas@manchester.ac.uk}
- Nikola Grunchevski  {nikola.grunchevski@manchester.ac.uk}
- Dirk Koch  {dirk.koch@manchester.ac.uk}