DETECTION OF COVERTLY EMBEDDED HARDWARE IN DIGITAL SYSTEMS
Hardware Tampering

- Software Attacks
  - Rootkits
  - Backdoors
  - Spyware
  - Key loggers
  - Viruses
  - List goes on and on…

- Hardware Attacks?
Main Idea

- Finite State Machine Model

Diagram:

- Circuit Inputs (I)
- Next State Logic (δ)
- State Memory (S)
- Output Logic (λ)
- Circuit Outputs (O)
Example - Stoplight
Example - Stoplight
Example - Stoplight

EECE Dept. Binghamton University 2/25/2011
One Hot State Encoding

Unused State Codes

<table>
<thead>
<tr>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
</tr>
<tr>
<td>011</td>
</tr>
<tr>
<td>101</td>
</tr>
<tr>
<td>110</td>
</tr>
<tr>
<td>111</td>
</tr>
</tbody>
</table>
Reprogrammable Devices

- FPGA (Field Programmable Gate Arrays)
  - Speed optimization
  - Area constraints

- LUT (Look up tables)
People Involved with Research

- Professor Summerville
  - Jim Moronski (PhD)
  - Qiong Gui (PhD)
    - Justin VanTassel (MS)
    - Alex Pang (MS)
    - Kyle Temkin (BS)
    - Ivan Sekyonda (BS)
    - Nick Tangchakkrachai (BS)
Questions/Comments

- Email: jvantas1@binghamton.edu