Remote Activation of ICs for Piracy Prevention and Digital Rights Management

Yousra Alkabani \(^1\)
Farinaz Koushanfar \(^1\)
Miodrag Potkonjak \(^2\)
\(^1\)Rice University and \(^2\)UCLA

Outline

- Introduction
- Related work
- Remote IC activation
- Attacks and countermeasures
- Experimental results
- Conclusion
Introduction

- Horizontal business model
- Pros and Cons
  - No designer control (asymmetric relationship)
  - Opaque ICs’ internals
  - Fabrication facilities with significant resources
  - The mask is expensive, but once made reproduction of the IC is cheap

HW metering

- A set of protocols to control the number of produced ICs
- Passive metering
  - Uniquely identify each chip
  - Register the unique ID of each chip
  - Suspicious ICs will be checked for their IDs
- Active metering
  - Actively control, enable and authorize each manufactured IC
Flow

Designer Alice

Design specification

Modified FSM

RTL synthesis, mapping, place & route

Manufacturing process

GDSII + test vectors

Disabled IC

Scan the unique locked states

Key calculation

Lock value

Enable and activate

Alice gains control over the number of functional chips produced

FSM modification

Input

Original FSM

Output

- A sequence of Inputs leads to functional transitions
- Correct transitions give functional output
The original sequence of Inputs leads to incorrect transitions
Incorrect transitions giving incorrect output

The chip will not function correctly UNLESS...

- Using the correct key
- A correct sequence of Input leads to correct transitions
- Correct transitions give correct output
Outline

* Introduction
* Related work
* Remote IC activation
* Attacks and countermeasures
* Experimental results
* Conclusion

Related Work

* Unique ID per chip
  * Manufacturer variability [Lofstrom et al. 2000, Su et al. 2007]
  * Passive metering [Koushanfar et al. 2001]
* Physically unclonable functions
  * Challenge response [Gassend et al. 2004, Lee et al. 2004]
* The first active hardware metering scheme
  * Boosted FSMs [Alkabani & Koushanfar 2007]
  * Locked/unlocked activation by moving to the reset state
* Our scheme is a novel method that actively controls many intermediate states
Outline

- Introduction
- Related work
- Remote IC activation
- Attacks and countermeasures
- Experimental results
- Conclusion
Modification of FSM

- Pick n states
- For every state $S_i$
  - Replicate all transitions as function of subset of the RUB m times

RUB output: $a, b$
Key: $k$, $f = \text{xor}(k, b)$

The Unclonable Random Unique Block (RUB)

- More randomness
- Nonlinearity

[Dijk et al., 2004]
**Augmentation of STG**

- Transitions to replicated states
  - Function of the RUB
- Transitions from replicated states
  - Function of both the RUB and the Key
  - Example: XOR RUB and Key bits

**Outline**

- Introduction
- Related work
- Remote IC activation
- Attacks and countermeasures
- Experimental results
- Conclusion
Attacks

- Brute force attack
  - Application of random inputs hoping it will produce the right input
- Reverse engineering of STG
- Combinational redundancy removal
  - Removal of unnecessary logic
- RUB emulation
  - Construct circuits that give identical performance

Countermeasures

- Brute force attack
  - The probability of achieving the correct input is going exponentially low with increasing the number of replicated states
  - Black-holes can be added to make this attack more difficult
- Reverse engineering of STG
  - The extraction of the STG is a computationally intractable task – 100s of FFs on average
- Combinational redundancy removal
  - The added states affect the functionality of the circuit. Thus, they cannot be considered as redundant
- RUB emulation
  - The RUB is unclonable
Outline

- Introduction
- Related work
- Remote IC activation
- Attacks and countermeasures
- Experimental results
- Conclusion

Experimental results

- Simulation using Berkeley SIS
- Using MCNC’91 benchmarks
- Choosing a state to replicate
  - Random
  - Heuristic: Pick the state with the least number of outgoing edges
### Area overhead

<table>
<thead>
<tr>
<th>BM</th>
<th>PI</th>
<th>States</th>
<th>Area (lits)</th>
<th>area</th>
<th>% area</th>
<th>Area (lits)</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>planet</td>
<td>7</td>
<td>48</td>
<td>888</td>
<td>1,373</td>
<td>54.6</td>
<td>1,191</td>
<td>34.12</td>
</tr>
<tr>
<td>s510</td>
<td>19</td>
<td>47</td>
<td>605</td>
<td>1,005</td>
<td>66.1</td>
<td>987</td>
<td>63.14</td>
</tr>
<tr>
<td>sand</td>
<td>11</td>
<td>32</td>
<td>1,092</td>
<td>3,851</td>
<td>253</td>
<td>1,634</td>
<td>49.63</td>
</tr>
<tr>
<td>s1488</td>
<td>8</td>
<td>48</td>
<td>880</td>
<td>2,457</td>
<td>179</td>
<td>1,248</td>
<td>41.82</td>
</tr>
<tr>
<td>s1494</td>
<td>8</td>
<td>48</td>
<td>859</td>
<td>2,655</td>
<td>209</td>
<td>1,276</td>
<td>48.54</td>
</tr>
<tr>
<td>Avg.</td>
<td></td>
<td></td>
<td></td>
<td>138.4</td>
<td></td>
<td>77.54</td>
<td></td>
</tr>
</tbody>
</table>

### Power and delay overhead

<table>
<thead>
<tr>
<th>BM</th>
<th>D (ms)</th>
<th>P (mW)</th>
<th>D (%)</th>
<th>P (%)</th>
<th>D (%)</th>
<th>P (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>planet</td>
<td>186.2</td>
<td>3,087</td>
<td>-49.57</td>
<td>60.77</td>
<td>-63.64</td>
<td>41.68</td>
</tr>
<tr>
<td>s510</td>
<td>47.6</td>
<td>2,280</td>
<td>70.38</td>
<td>70.90</td>
<td>48.95</td>
<td>53.02</td>
</tr>
<tr>
<td>sand</td>
<td>74.80</td>
<td>3,917</td>
<td>18.72</td>
<td>265.4</td>
<td>-17.78</td>
<td>55.31</td>
</tr>
<tr>
<td>s1488</td>
<td>134.9</td>
<td>3,011</td>
<td>-32.25</td>
<td>186.9</td>
<td>-35.73</td>
<td>47.81</td>
</tr>
<tr>
<td>S1494</td>
<td>115.6</td>
<td>2,958</td>
<td>24.22</td>
<td>219</td>
<td>-26.82</td>
<td>54.15</td>
</tr>
<tr>
<td>Avg.</td>
<td></td>
<td></td>
<td>3.68</td>
<td>148.9</td>
<td>-11.39</td>
<td>83.95</td>
</tr>
</tbody>
</table>
Scalability analysis

![Graph showing scalability analysis]

Conclusion

- The first continuous IC authentication scheme
- Merging manufacturing variability with the functionality
- Different attacks on the scheme are discussed and countermeasures are added
- Experimental results on different benchmarks showed the method has low timing overhead