Research Project Proposal: IP Protection through Logic Locking at Register-Transfer Level

Luca Collini
luca.collini@mail.polimi.it
CSE
Outline

• Introduction to the problem
  ▪ Globalization of the IC supply chain & security threats
  ▪ Logic locking

• Research goal

• State of the art

• Research plan
Globalization of the IC supply chain

Design House

- High-level Spec.
- Params
- Manual Design
- Hardware Generators
- RTL Spec.
- Logic Synthesis
- Gate-level Spec.
- Physical Design
- Layout Spec.
- Fabrication

Untrusted foundry

- Legal IC Copies
- Illegal IC Copies

- Cost for a new foundry at 7 nm nodes: $5 billion
Security threats

Reverse Engineering

Intellectual Property theft
- estimated loss due to IP violations alone was $4 billions in 2008
- total loss from IC counterfeiting was estimated to be about $169 billions in 2011

Malicious modifications
- backdoor insertion
- planned obsolescence trojans
Logic Locking

Thwarting reverse engineering

Original Design

Logic Locking

Obfuscated Design

Key
011001111101110
101100110011010...

Unknown to the foundry
Logic Locking

Plain design

Obfuscated design

Shamsi, K., Li, M., Plaks, K., Fazzari, S., Pan, D. Z., and Jin, Y. Ip protection and supply chain security through logic obfuscation: A systematic overview
Logic Locking

Obfuscated Design

Key
0110011111101110
101100110011010...

Correct functionality

Wrong Key
1101010111010010
00101100011001...

Incorrect functionality
Outline

• Introduction to the problem
  ▪ Globalization of the IC supply chain & security threats
  ▪ Logic locking

• Research goal

• State of the art

• Research plan
Research goal

- High level approach to logic locking
- Quantitative metrics to compare different designs
Outline

• Introduction to the problem
  ▪ Globalization of the IC supply chain & security threats
    ▪ Logic locking

• Research goal

• State of the art

• Research plan
State of the art

**Threat model**: defines goals and abilities of the attackers

Logic locking threat models

- *Oracle*: a chip that performs correct computations
- *Ambiguity*: ability of an attacker to distinguish between primary inputs and key inputs

Common threat models:

- *Distinct ambiguity oracle-guided*: commercial products
- *Distinct ambiguity oracle-less*: low volume chips
## State of the art

### Evaluation metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification failure</td>
<td>Measures how the obfuscated design introduces failing points with wrong keys</td>
<td>Related to functionality</td>
</tr>
<tr>
<td>Entropy</td>
<td>Measures the number of distinct outputs of the circuit</td>
<td>Related to power and resiliency towards oracle-less attacks</td>
</tr>
<tr>
<td>Differential entropy</td>
<td>Measures the proportion of bits that differ between the obfuscated and the plain design</td>
<td>Related to power overhead</td>
</tr>
<tr>
<td>Reconvergence</td>
<td>Measures the rate of internal signals converging in other nodes</td>
<td>Related to resiliency towards key sensitization attack</td>
</tr>
<tr>
<td>Key structure metric</td>
<td>Measures the structural interconnection between the key gates</td>
<td>Related to resiliency towards key sensitization attack</td>
</tr>
</tbody>
</table>
State of the art

Pre-synthesis logic locking techniques

- TAO: HLS tool to produce obfuscated RTL descriptions
- ASSURE: pre-synthesis tool that works at RT level
- CDFG: RT level technique that obfuscates the data flow graph of a design
- BDD: pre-synthesis technique that works on Binary Decision Diagrams

Post-synthesis logic locking techniques

- RLL: random insertion of logic gates (typically XOR or XNOR gates) controlled by a key bit
- SLL: strengthens the insertion of logic gates by inserting key-gates with complex interference among them
- Anti-SAT: technique that aims at making SAT attacks unfeasible
- Cone size: integrates the key gates with other gates that have the largest fanin or fanout cone or both
## State of the art

<table>
<thead>
<tr>
<th>Method</th>
<th>Area overhead</th>
<th>Power overhead</th>
<th>Timing overhead</th>
<th>SAT attack resiliency</th>
<th>Key sens. attack resiliency</th>
<th>Verification failure metric</th>
<th>Entropy</th>
<th>Differential entropy</th>
<th>Reconvergence</th>
<th>Key structure metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDFG [2]</td>
<td>Low</td>
<td>Low</td>
<td>n.a</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
</tr>
<tr>
<td>BDD Random [4]</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>BDD AntiSAT [4, 12]</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>BDD Entropy [1]</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>RLL [8]</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>SLL [13]</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Cone size [1]</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>AntiSAT Random [8, 12]</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>AntiSAT SLL [13, 12]</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Anti SAT Cone size [1]</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
</tr>
</tbody>
</table>
## State of the art - Summary

<table>
<thead>
<tr>
<th>Category</th>
<th>Techniques</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-synthesis HLS</td>
<td>TAO, BDD</td>
<td>Hide semantic information</td>
<td>Require modification of the design flow</td>
</tr>
<tr>
<td>Pre-synthesis RTL</td>
<td>ASSURE, CDFG</td>
<td>Hide semantic information</td>
<td>?</td>
</tr>
<tr>
<td>Post-synthesis</td>
<td>RLL, SLL, Cone Size, Anti SAT</td>
<td>Do not require modifications on the design flow</td>
<td>Cannot protect information already embedded in the design by synthesis optimizations</td>
</tr>
</tbody>
</table>
State of the art

Conclusion

• ASSURE and CDFG showed that logic locking at register-transfer level deserves further investigations
• The proposed metrics are empiric and experimental and do not allow their use with optimization methods
• Hardware obfuscation is missing security properties clearly defined by mathematical terms

Open questions

• How to select obfuscation points?
• How to measure the security and compare two designs?
Outline

• Introduction to the problem
  ▪ Globalization of the IC supply chain & security threats
  ▪ Logic locking
• Research goal
• State of the art
• Research plan
Research plan

Research goal

develop a complete logic locking framework at register-transfer level

and

evaluate it with new security metrics
Research plan

We plan to carry out this research with a **two-phase development plan**

- **First development round**: prototype implementing the RTL obfuscation techniques and evaluation chain to measure cost and security

- **First evaluation round**: benchmarking the prototype using the evaluation chain

- **Second development round and final evaluation**: refining the techniques and the metrics identified in the first phase thanks to the evaluation feedback
Research plan

- **Sep**: State of the art analysis, SotA and PP
- **Oct**: First implementation round, Prototype
- **Nov**: Evaluation chain and metrics identification, Evaluation chain
- **Dec**: First evaluation
- **Jan**: Second implementation round
- **Feb**: Final evaluation
- **Mar**: Refined prototype/evaluation chain
- **Apr**: Thesis Writing

Legend:
- Theoretical task
- Implementation task
- Experimental task
Thank you for your attention!

Luca Collini

luca.collini@mail.polimi.it