Hardware IP Protection against Confidentiality Attacks and Evolving Role of CAD Tool (Invited Paper)

Author: Swarup Bhunia, Vivian Kammler, Amitabh Das, David Kehlet, Saverio Fazzari, Jeyavijayan Rajendran

Source: 2022 International Conference On Computer Aided Design (ICCAD)

Speaker: Kuan-Ting Chen
Outline

● Introduction
● Protection
● Attacks and Security analysis
● Conclusions
Introduction

3PIP1 -> License -> SoC Design -> Contract -> Chips

3PIP2 -> Sell -> SoC Designer

3PIPl -> Trust

... -> Trust

IP Owners

#chips

Foundry/Assembly
Introduction
Introduction

Reverse Engineering
1. De-packaging
2. Delayering
3. Imaging
4. Analyzing
# Protection

## Defense against Confidentiality Attacks

<table>
<thead>
<tr>
<th>Category</th>
<th>Passive Defense</th>
<th>Active Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defense Mechanism</td>
<td>Watermarking</td>
<td>Logic Locking</td>
</tr>
<tr>
<td></td>
<td>State Space Obfuscation</td>
<td>Hardware Redaction</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP Encryption (IEEE-1735-2014 std)</td>
</tr>
<tr>
<td>ASIC or FPGA Flow</td>
<td>ASIC, FPGA</td>
<td>ASIC</td>
</tr>
<tr>
<td></td>
<td>ASIC</td>
<td>ASIC</td>
</tr>
<tr>
<td>Protects against</td>
<td>Piracy</td>
<td>Piracy, RE, EDS</td>
</tr>
<tr>
<td></td>
<td>Piracy, RE, EDS</td>
<td>Piracy, RE, EDS</td>
</tr>
<tr>
<td></td>
<td>Piracy, RE, EDS</td>
<td>Piracy, RE, EDS</td>
</tr>
<tr>
<td></td>
<td>Piracy, RE, EDS</td>
<td>Piracy, RE, EDS</td>
</tr>
</tbody>
</table>
Watermarking

◆ Hard to identify
◆ Permanently embedded into an IP
◆ Hard to remove and tamper
◆ Easy to verify
◆ Incurs low cost
◆ Remains invariant to design transformation
Logic locking
State Space Obfuscation
State Space Obfuscation

AES-128

0.1 * 2^{270}

0.8 * 2^{276}
Hardware Redaction

◆ Remove logic from a design
◆ Replace them with lookup tables (LUTs) and a bitstream
Hardware Redaction

◆ Which module(s) should a designer redact?
◆ What is the impact of inserting eFPGAs into the ASIC design flow?
◆ How can the designer generate the proper eFPGA architecture?
◆ Are all eFPGA architectures equally secure?
IP Encryption

- SystemVerilog
- Verilog
- VHDL

IEEE-1735-2014
Attacks and Security analysis

- Gate-level netlist
- Oracle (oracle-guided attack)
- Scan-chain
Security metrics

◆ The common metrics used for overhead analysis are impact on PPA values
◆ There is no “golden” metric for security
◆ The metric must be acceptable to the community for usage
◆ The security metrics fall into two broad categories
  ◆ Brute-force attack complexity
  ◆ Practical attack complexity
Salient Attacks on Protected IPs

Functional
◆ SAT attack
◆ SWEEP

Structural
◆ SAIL attack
◆ SnapShot
Conclusions

◆ Protecting hardware IP blocks is a major concern for vendors and designers.
◆ The modern hardware supply chain involves many untrusted parties, challenging hardware IP protection.
◆ EDA companies are expected to integrate design and verification solutions for IP protection.
◆ Machine learning may help develop robust protection methodologies to resist known and future attacks.