Complete Activation Scheme for IP Design Protection

Brice Colombier, Ugo Mureddu, Oto Petura, Lilian Bossuet, Viktor Fischer
Univ. Lyon, UIM-Saint-Etienne, CNRS
Laboratoire Hubert Curien UMR 5516
F-42023, Saint-Etienne, France

Marek Laban
Department of Electronics and Multimedia Communications,
Technical University of Kosice, Park Komenskho 13
04120 Kosice, Slovak Republic,
MICRONIC, Silacska 2/C, 83102, Bratislava, Slovak Republic

David Hély
Univ. Grenoble Alpes, LCIS
F-26000, VALENCE, France

**Current situation**
- Integrated circuits are increasingly complex,
- Core-based design is the norm,
- Design data transfer is necessary,
- Illegal copying and overusing are rising.

**Implementation results**

<table>
<thead>
<tr>
<th>Component</th>
<th>6-LUTs</th>
<th>DFFs</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUF</td>
<td>4841</td>
<td>32</td>
</tr>
<tr>
<td>Controller</td>
<td>104</td>
<td>90</td>
</tr>
<tr>
<td>MUXes (parities &amp; indexes)</td>
<td>338</td>
<td>0</td>
</tr>
<tr>
<td>Parity computation module</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>AW sampler</td>
<td>0</td>
<td>128</td>
</tr>
<tr>
<td>Parity shift register</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td>Response shift register</td>
<td>0</td>
<td>128</td>
</tr>
</tbody>
</table>

**Proposed solution**

Make the design remotely activable.
Requirements:
- Unique identifier for each instance,
- Two modes of operation (disabled and normal),
- Mid-term security.
Characteristics:
- Lightweight,
- Easy to integrate into EDA tools,
- Usable with all types of designs.

- Balanced level of protection during operation (without wasting performance in normal mode)
- Secure design
- Easy to integrate into EDA tools
- Usable with all types of designs

**Overall Architecture**

- **Logic locking**
  - Integrates a lightweight block cipher
  - Brings high-level security

- **Logic masking**
  - Use of a masking module
  - Combines lightweight security with high-level security

- **TERO-PUF**
  - Protects IP blocks
  - Combines lightweight security with high-level security

- **CASCADE key reconciliation**
  - Use of a secret key
  - Ensures secure key distribution

**Logic locking**

- **Centrality indicators as the node selection heuristic**
  - Example: Current-flow betweenness centrality
  \[ \gamma_{BF}(v) = \sum_{s \neq v \neq t} \rho((s, v) \rightarrow (v, t)) \]

- **Masking efficiency metric**
  \[ \psi_{M}(n) = \sum_{n \in \text{neighbours}} \rho^2(\text{normal} \rightarrow \text{masked}) \]

**Logic masking**

- Use of a masking module
- Combines lightweight security with high-level security

**TERO-PUF**

- Protects IP blocks
- Combines lightweight security with high-level security

**CASCADE key reconciliation**

- Use of a secret key
- Ensures secure key distribution

**Contact**

b.colombier@univ-st-etienne.fr
www.univ-st-etienne.fr/salware/