Let's Tessellate: Tiling for Security Against Advanced Probe and Fault Adversaries

Joint work with Siemen Dhooghe and Svetla Nikova
Security models: what do we need?

- Easy verification: composable security
- Capture of leakage effects
- Allows for efficient countermeasures
Probe Model

* Private Circuits: Securing Hardware against Probing Attacks: Yuval Ishai, Amit Sahai, David Wagner
Robust Probe Model: Glitches

* Composable Masking Schemes in the Presence of Physical Defaults and the Robust Probing Model, Sebastian Faust, Vincent Grosso, Santos Merino Del Pozo, Clara Paglialonga, François-Xavier Standaert
Robust Probe Model: Transitions

* Composable Masking Schemes in the Presence of Physical Defaults and the Robust Probing Model, Sebastian Faust, Vincent Grosso, Santos Merino Del Pozo, Clara Paglialonga, François-Xavier Standaert
Robust Probe Model: Couplings

* Composable Masking Schemes in the Presence of Physical Defaults and the Robust Probing Model, Sebastian Faust, Vincent Grosso, Santos Merino Del Pozo, Clara Paglialonga, François-Xavier Standaert
Wire Fault Model
Extended Fault Model: Area Faults
Extended Fault Model: Permanent Faults
Tile Model and CAPA
Tile Model and CAPA
Tile Model and CAPA

\[ T_1 \]

\[ T_2 \]

\[ T_3 \]
Relation Between Probe and Fault Models

- Probing Model
- Wire Fault Model
- Robust Probing Model
- Extended Fault Model
- Tile Probing Model
- Tile Fault Model

**Stronger Model:**
Providing security against more leakage effects
Comparing Compositional Notions
# shares/duplicates required for \((d, k)^{th}\)-order security

<table>
<thead>
<tr>
<th></th>
<th>NI &amp; NA</th>
<th>Standalone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Glitches</td>
<td>(d+1)</td>
<td>(d+1)</td>
</tr>
<tr>
<td>Transitions</td>
<td>(2d+1)</td>
<td>(d+1)</td>
</tr>
<tr>
<td>Couplings</td>
<td>(d+1)</td>
<td>(d+1)</td>
</tr>
<tr>
<td>Area Faults</td>
<td>(k+1)</td>
<td>(k+1)</td>
</tr>
<tr>
<td>Permanent Faults</td>
<td>(2k+1)</td>
<td>(k+1)</td>
</tr>
</tbody>
</table>
A Tiled ISW Method
A Tiled ISW Method
Table 2. Comparison of CAPA and this work’s multipliers for practical parameters. The scheme of CAPA has a $|\mathbb{F}|^{-m}$ probability of a fault breaking its security, while Alg. 6 always guarantees security.

<table>
<thead>
<tr>
<th>Alg.</th>
<th>$d, k, m = 1$</th>
<th>$d, k, m = 2$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$\times$</td>
<td>$+$</td>
</tr>
<tr>
<td>Alg. 6</td>
<td>8</td>
<td>36</td>
</tr>
<tr>
<td>CAPA</td>
<td>48</td>
<td>78</td>
</tr>
</tbody>
</table>
Conclusion

- Extension of the fault model
- Comparison with the tile model
- Proposal of tiled ISW method