Composable Gadgets with Reused Fresh Masks - First-Order Probing-Secure Hardware Circuits with only 6 Fresh Masks

David Knichel and Amir Moradi

CHES, September 2022, Leuven, Belgium
CONTRIBUTION

What is it all about?

We've built a hardware gadget

- Enable the composition of any first-order (glitch-extended) robust secure circuit
- No gadget-individual fresh randomness necessary
- Only 6 fresh random masks in total
- Leads to randomness-optimized designs
- **COMAR** (Composable Gadgets with Reused fresh Masks)
STATUS QUO

What do we have?

Masking on an algorithmic Level

- Requires high expertise
- Prone to errors
- Often no formal security proof
- Leads to optimized designs

Gadget-based Masking

- Based on composability notions
- Can be automated
- Leads to provable secure designs
- Usually introduces higher overhead
ADVERSARY MODEL

What can an SCA adversary observe?

The ISW d-probing model

- Offers high abstraction
- Existing reduction into the Noisy Leakage Model (which is close to the real world)
- Extension to HW: robust d-probing Model
ADVERSARY MODEL

Glitch-extended robust probing model
PROBLEM

Why is our work important?

Composable gadgets are typically realizing atomic gates

• AND, OR, NAND, NOR, ...

This introduces individual randomness overhead per gadget

• Results in high overall overhead w.r.t. the randomness requirements
RESEARCH QUESTION

What was the goal?

Can we build gadgets where we can re-use the same randomness in every gadget?
What was the goal?
Gadget-individual fresh mask allow to argue about simulatability of probes within a gadget because the input is independent of any other fresh mask.

Why is fresh randomness necessary?
Our AND gadget

\[ A^0 \rightarrow R_0 \rightarrow A^1 \rightarrow R_1 \rightarrow B^0 \rightarrow R_1' \rightarrow B^1 \rightarrow R_2 \rightarrow R_0' \rightarrow C^0 \rightarrow C^1 \]

\[ R_0' \rightarrow R_1' \rightarrow R_2' \rightarrow R_3' \]
Our XOR gadget

\[
\begin{align*}
A^0 & \rightarrow R_0 \\
A^1 & \rightarrow R_1 \\
B^0 & \rightarrow R_1 \\
B^1 & \rightarrow R_3
\end{align*}
\]

\[
\begin{align*}
R_0' & \rightarrow R_0 \\
R_1' & \rightarrow R_1 \\
R_2' & \rightarrow R_2 \\
R_3' & \rightarrow R_3
\end{align*}
\]

\[
\begin{align*}
C^0 & \rightarrow R_0 \\
C^1 & \rightarrow R_1
\end{align*}
\]
We can extend our 2-input gadgets

We also constructed n-input ANDs

- and all other non-linear gates which can easily be derived from AND

\[ n + 2^n \] fresh masks are needed for the whole circuit.

- Here \( n \) is the maximal input width used within the circuit.
Is it worth it?

The randomness requirements are drastically improved by our approach

- Breakeven point compared to for example HPC2 is 6 AND gates

Additional latency is the price we pay here

- XOR is not for free w.r.t. latency as for example in the PINI framework

Multiple-input gadgets mitigate this disadvantage
Let's see some results

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>added</td>
<td>full</td>
<td></td>
</tr>
<tr>
<td>AES-128</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HPC2</td>
<td>680</td>
<td>8</td>
<td>99</td>
<td>2.04</td>
</tr>
<tr>
<td>GHPC</td>
<td>680</td>
<td>8</td>
<td>99</td>
<td>1.48</td>
</tr>
<tr>
<td>GHPC&lt;sub&gt;LL&lt;/sub&gt;</td>
<td>2720</td>
<td>4</td>
<td>55</td>
<td>2.28</td>
</tr>
<tr>
<td>COMAR</td>
<td>6</td>
<td>42</td>
<td>473</td>
<td>1.23</td>
</tr>
<tr>
<td>Skinny64-64</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HPC2</td>
<td>64</td>
<td>4</td>
<td>165</td>
<td>0.55</td>
</tr>
<tr>
<td>GHPC</td>
<td>64</td>
<td>2</td>
<td>99</td>
<td>0.80</td>
</tr>
<tr>
<td>GHPC&lt;sub&gt;LL&lt;/sub&gt;</td>
<td>1024</td>
<td>1</td>
<td>66</td>
<td>0.85</td>
</tr>
<tr>
<td>COMAR</td>
<td>6</td>
<td>22</td>
<td>759</td>
<td>0.58</td>
</tr>
</tbody>
</table>
### CASE STUDIES

Considering the randomness source

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Area [GE]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LFSR 31-bit</td>
</tr>
<tr>
<td><strong>AES-128</strong></td>
<td></td>
</tr>
<tr>
<td>HPC2</td>
<td>247 281</td>
</tr>
<tr>
<td>GHPC</td>
<td>261 673</td>
</tr>
<tr>
<td>GHPC\textsubscript{LL}</td>
<td>830 370</td>
</tr>
<tr>
<td>COMAR</td>
<td>141 932</td>
</tr>
<tr>
<td><strong>Skinny64-64</strong></td>
<td></td>
</tr>
<tr>
<td>HPC2</td>
<td>25 218</td>
</tr>
<tr>
<td>GHPC</td>
<td>41 154</td>
</tr>
<tr>
<td>GHPC\textsubscript{LL}</td>
<td>311 569</td>
</tr>
<tr>
<td>COMAR</td>
<td>23 808</td>
</tr>
</tbody>
</table>

Composable Gadgets with Reused Fresh Masks

CHES, September 2022, Leuven, Belgium
Thanks!
Any Questions?
david.knichel@rub.de