Secure and Reliable XOR Arbiter PUF Design: An Experimental Study based on 1 Trillion Challenge Response Pair Measurements

Chen Zhou, Keshab K. Parhi, Chris H. Kim

University of Minnesota, Minneapolis, MN, USA
zhoux825@umn.edu
**Single MUX Physical Unclonable Function (PUF)**

- **Advantage:**
  - Large # of challenge response pairs (CRPs): $2^n$

- **Disadvantages:**
  - Stability: responses sensitive to noise, VDD & temperature variation.
  - Security: delay parameters can be extracted easily through linear additive model

\[
\begin{align*}
C &= \begin{bmatrix}
(2c_1 - 1)(2c_2 - 1) \cdots (2c_n - 1) \\
(2c_2 - 1) \cdots (2c_n - 1) \\
\vdots \\
(2c_n - 1)
\end{bmatrix}^T \\
W &= \frac{1}{2} \begin{bmatrix}
\delta_0^0 - \delta_1^1 \\
\delta_1^0 + \delta_1^1 + \delta_2^0 - \delta_2^1 \\
\vdots \\
\delta_n^0 + \delta_n^1 + b
\end{bmatrix}
\end{align*}
\]

\[
\Delta = C \cdot W
\]

\[
\text{response} = (\text{sign}(\Delta) + 1) / 2
\]

J. Delvaux, et al., HOST, 2013
XOR MUX PUF

Advantages:
- Internal responses hidden
- Linear additive model not applicable
- Simple implementation

Disadvantage:
- Poor stability

Single MUX PUF
- Input challenge → PUF → Response
  - Visible to hacker

XOR MUX PUF
- Input challenge (shared) → PUF #1 → Response #1
- PUF #2 → Response #2
- PUF #3 → Response #3
- ⋮
- PUF #n → Response #n
  - n-input XOR → Final response

Invisible to hacker
- Visible to hacker

<table>
<thead>
<tr>
<th>PUF</th>
<th>Response</th>
<th>Stability</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUF #1</td>
<td>Response #1</td>
<td>Stable</td>
</tr>
<tr>
<td>PUF #2</td>
<td>Response #2</td>
<td>Stable</td>
</tr>
<tr>
<td>PUF #3</td>
<td>Response #3</td>
<td>Unstable</td>
</tr>
<tr>
<td>⋮</td>
<td>⋮</td>
<td>⋮</td>
</tr>
<tr>
<td>PUF #n</td>
<td>Response #n</td>
<td>⋮</td>
</tr>
</tbody>
</table>

Final response
- Stable
- Stable

XOR

Stable final response

Stable

Stable

Stable

Stable

Stable

Stable

Stable

Stable
XOR MUX PUF Security

- 1,000,000 CRPs collected in 32nm chip
- 3-layer perceptron classifier used
- $n>10$ required for sufficient security
XOR MUX PUF Stability

- **Single MUX PUF**
  - Soft response based on 100,000 repetitive tests
  - 79.8% of CRPs are stable (in 1 million tested CRPs)

- **XOR PUF**
  - All $n$ responses must be stable
  - $\sim (80\%)^n$ of CRPs yield stable final responses
Proposed XOR PUF Enrollment Method

- Counters measure soft responses
- Linear model and thresholds extracted
- Fuses blown out

Measure Soft Response of Individual PUF
- Challenges → PUF → Soft responses
- Extract Delay Parameters
- Challenges → Linear regression → Trained model
- Determine Threshold
- Prediction → Compare → Model thresholds
- Burn Fuses Before Deployment
Proposed XOR PUF Authentication

- Challenges selected by models
- 100% match required to authorize access
Model Threshold Determination

- Thresholds help find stable CRPs
- Measurement vs. model prediction:
  - Both responses centered at 0.5
  - Strong correlation
  - Threshold levels optimized

![Diagram showing soft response measurement and prediction with thresholds for selecting stable '0' and '1' responses.](image_url)
Thresholds Adjustment

• Response variation expanded:
  – Test set CRPs not trained
  – VDD and temperature variation
Advantage of Model based CRP Selection

- **Measurement based CRPs selection:**
  - Stable and marginally stable CRPs indistinguishable
  - Large enrollment set size

- **Model based CRPs selection:**
  - Linearly related to delay difference
  - Captures detailed stability information
  - Modest enrollment set size: ~5,000 CRPs
• Percentage of stable CRPs:
  – 80.0%: measured under *nominal* VDD and temperature
  – 54.5%: model predicted under *nominal* VDD and temperature
  – 34.2%: model predicted under *variable* VDD and temperature

• Stable CRPs in 10-input XOR PUF (0.8V~1.0V, 0~60ºC): 0.0028%
Summary

• Security and stability of XOR PUF evaluated using 1 trillion CRP data measured from 32nm test chips
• Secure XOR PUF should have $n > 10$
• A linear regression model helps select stable CRPs
• Stringent thresholds used to compensate for V and T variation

Acknowledgements

• National Science Foundation and Semiconductor Research Corporation for funding