Soft Response Generation and Thresholding Strategies for Linear and Feed-Forward MUX PUFs

Chen Zhou, Saroj Satapathy, Yingjie Lao, Keshab K. Parhi and Chris H. Kim

Department of ECE
University of Minnesota
Outline

• Physical Unclonable Function (PUF)
• 32nm PUF Chip Measurements
• Soft Response Thresholding Strategies
• Linear PUF vs. Feed-forward PUF
• Conclusion
Physical Unclonable Function (PUF)

- Unique and random: Based on inherent process variation
- Secure: Large # of challenge-response pairs (CRPs)

![PUF Diagram]

Fingerprint of chip

Numerous input choices

Inputs
- Challenge #1
- Challenge #2
- ...
- Challenge #n

Outputs
- Response #1
- Response #2
- ...
- Response #n

Unique and random responses

Challenges

Chip #1
- Responses #1

Chip #2
- Responses #2

≠
• Server-user based authentication
• Challenge-response pairs tested and stored before usage
Typical Authentication Process

- Public chip ID is first sent to the server
Typical Authentication Process

- Server retrieves CRP subset table for the given chip ID

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>209A (Hex)</td>
<td>0</td>
</tr>
<tr>
<td>41B1 (Hex)</td>
<td>1</td>
</tr>
<tr>
<td>9283 (Hex)</td>
<td>1</td>
</tr>
</tbody>
</table>

Server User

Database

Retrieve CRP subset
**Typical Authentication Process**

- Challenges are sent to the user

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>209A (Hex)</td>
<td>0</td>
</tr>
<tr>
<td>41B1 (Hex)</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>9283 (Hex)</td>
<td>1</td>
</tr>
</tbody>
</table>
• User generates responses using PUF circuit
Typical Authentication Process

- User responses are sent to server for comparison
Typical Authentication Process

- **Approved if responses match; denied if mismatch**
- **Final step: decision sent to user**
Hamming Distance (HD) Calculation

- Hamming distance can be used as matching criteria
- Intra-chip HD: Same chip, noise effects, close to 0%
- Inter-chip HD: Different chip, process variation effects, close to 50%
Outline

• Physical Unclonable Function (PUF)

• 32nm PUF Chip Measurements

• Soft Response Thresholding Strategies

• Linear PUF vs. Feed-forward PUF

• Conclusion
Motivation of This Work

- Stable CRPs have less intra-chip variation
- Measure soft response (=probability of response being ‘1’ or ‘0’) to find stable CRPs

Actual case (only stable CRPs)
Contributions of This Work

• Implemented soft response collection circuits in a 32nm test chip

• Generated MUX PUF soft response distribution based on 3.3 Gb test data

• Proposed soft response thresholding strategies to select stable challenge-response pairs

• Implemented and characterized feed-forward MUX PUF
Proposed Soft Response Measurement Circuit

- Soft response = response probability information
- >GHz sampling circuits facilitate efficient soft response measurements
Linear MUX PUF Delay Stages

- Parallel or crossed signal paths configured by challenge bits
- Delay difference determined by inherent process variation
Arbiter Circuit

- Arbiter generates response bit based on delay difference
### 32nm PUF Test Chip

#### Diagram:
- **Dimensions:** 494um x 750um
- **Features:**
  - DCAP
  - Linear MUX arbiter PUF (48 instances)
  - Feed-forward MUX arbiter PUF (48 instances)
  - SCAN CHAIN
  - VCO

#### Specifications:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process</strong></td>
<td>32nm</td>
</tr>
<tr>
<td><strong>VDD</strong></td>
<td>0.8V, 0.9V, 1.0V (nominal: 0.9V)</td>
</tr>
<tr>
<td><strong>Temperature</strong></td>
<td>25°C, 85°C</td>
</tr>
<tr>
<td><strong>Circuit area</strong></td>
<td>0.37 mm²</td>
</tr>
<tr>
<td><strong>PUF type</strong></td>
<td>Linear and Feed-forward MUX arbiter PUF</td>
</tr>
<tr>
<td><strong>PUF stages</strong></td>
<td>32</td>
</tr>
<tr>
<td><strong># of PUFs</strong></td>
<td>48 (linear) + 48 (feed-forward)</td>
</tr>
<tr>
<td><strong>VCO frequency</strong></td>
<td>&lt;1.4 GHz</td>
</tr>
<tr>
<td><strong>Arbiter</strong></td>
<td>SR latch</td>
</tr>
</tbody>
</table>
Soft response is a function of the actual delay difference

Above distribution generated using 3.3 Gb of PUF response data
Outline

• Physical Unclonable Function (PUF)

• 32nm PUF Chip Measurements

• Soft Response Thresholding Strategies

• Linear PUF vs. Feed-forward PUF

• Conclusion
Soft Response Thresholding Strategy

100k samples, 0.9V, 25°C

- $\Pr(\text{stable} \ '0') = 48.24\%$
- $\Pr(\text{stable} \ '1') = 45.92\%$
- $\Pr(\text{unstable}) = 5.84\%$

Threshold for '0' = 0.2
Threshold for '1' = 0.8

Authentication with stable CRPs

- Database responses
- User responses
- Unstable CRP
- Hamming distance: % of mismatch

- Symmetric thresholds used to define stable and unstable CRPs
- Unstable CRPs not used for authentication
Impact of Soft Response (SR) Threshold

VDD: 0.8, 0.9, 1.0V  Temperature: 25, 85°C  64 stable CRPs  32nm data

- Left: HD distributions overlap when threshold=0.5
- Right: No overlap when threshold=0 and 1 (i.e. only stable responses are used)
- No stable ‘1’ to stable ‘0’ flips when threshold > 0.81
- Stable ‘1’ to ‘unstable’ flips always exist, necessitating more tests to find stable CRPs
Relaxed Threshold Scheme

- Stringent threshold during enrollment phase and relaxed threshold during authentication
- Results in fewer ‘1’→’unstable’ and ‘0’→’unstable’ flips
Outline

• Physical Unclonable Function (PUF)

• 32nm PUF Chip Measurements

• Soft Response Thresholding Strategies

• Linear PUF vs. Feed-forward PUF

• Conclusion
Linear MUX PUF Vulnerability

C = \begin{bmatrix}
(2c_1 - 1)(2c_2 - 1) \cdots (2c_{32} - 1) \\
(2c_2 - 1) \cdots (2c_{32} - 1) \\
\vdots \\
(2c_{32} - 1)
\end{bmatrix}^T

W = \frac{1}{2} \begin{bmatrix}
\delta^0_1 + \delta^1_1 + \delta^0_2 - \delta^1_2 \\
\delta^0_{31} + \delta^1_{31} + \delta^0_{32} - \delta^1_{32} \\
\delta^0_{32} + \delta^1_{32} + b
\end{bmatrix}

\Delta = C \cdot W

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

- Linear PUFs are susceptible to modelling attack
- That is, attacker can predict correct response with very high probability using past CRP data
Feed-forward MUX PUF for Improved Security

- Use intermediate response for some challenge bits
- Non-linear relationship between delay and response → harder for attacker to predict correct response
- No experimental data reported on feed-forward PUF

Feed-forward MUX PUF ref.: J. W. Lee, et al., VLSI Circuits Symposium, 2004
32nm Test Chip Data: Linear vs. Feed-forward MUX PUF

- % of stable CRPs decreases from 94.16% to 91.02% due to instability of internal challenge bit
Conclusion

• Soft response measurement circuit demonstrated in a 32nm test chip
  – On-chip VCO and counters enable fast measurement

• Different thresholding strategies evaluated
  – Enables robust authentication across wider voltage and temperature range

• Feed-forward MUX measured for the first time
  – % of stable CRPs decreases slightly due to instability of internal challenge bit

Acknowledgements

• National Science Foundation and Semiconductor Research Corporation for funding