XOR Arbiter PUFs have Systematic Response Bias

Nils Wisiol and Niklas Pirnay

Financial Cryptography 2020 · Kota Kinabalu · 10 Feb 2020
nils.wisiol@tu-berlin.de · niklas.pirnay@campus.tu-berlin.de
How To Start Your Financial Crypto 2020
Card Verification with PKI

- Secret key
- Nonce etc.
- Signature
- Public key
Card Verification with PUFs

challenge

response

<table>
<thead>
<tr>
<th>challenge</th>
<th>response</th>
</tr>
</thead>
<tbody>
<tr>
<td>101000111</td>
<td>1001110</td>
</tr>
<tr>
<td>100111001</td>
<td>1010101</td>
</tr>
<tr>
<td>100011111</td>
<td>1100000</td>
</tr>
<tr>
<td>101010011</td>
<td>1010101</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
Arbiter PUF 101

\[ c_1^{(1)} = +1 \]
\[ c_2^{(1)} = -1 \]

\[ c_{n-1}^{(1)} \quad c_n^{(1)} \]
Arbiter PUF Variants: XOR Arbiter PUF

History of Arbiter-based PUFs
Interpose PUFs

\[ k_{up} \]

\[ f_u(c) \]

\[ k_{down} \]

\[ f(c) \]
Lightweight Secure PUF

Majzoobi, Mehrdad, Farinaz Koushanfar, and Miodrag Potkonjak.
Permutation PUF
XOR Arbiter PUFs have Systematic Response Bias
Proportion of XOR Arbiter PUFs that Pass NIST Test
Proportion of XOR Arbiter PUFs that Pass NIST Test
Conclusion for Novel Designs
Keep the Bias in Mind
Thank You!

All data and code freely available in pypuf:

github.com/nils-wisiol/pypuf

nils.wisiol@tu-berlin.de

ia.cr/2019/1091

XOR Arbiter PUFs have Systematic Response Bias

Short Paper

Nils Wisiol · {Freie, Technische} Universität Berlin
Niklas Pirnay · Technische Universität Berlin
Arbiter PUF Models

\[ r(c) = \text{sgn} \left[ \langle w, x \rangle + w_0 \right] = \text{sgn} \left[ \left( \sum_{i=1}^{n} w_i x_i \right) + w_0 \right] \]

\[ r(c) = \text{sgn} \left( \prod_{l=1}^{k} \sum_{i=1}^{n} w_{l,i} x_i + w_{l,0} \right) \]