The Wiretap Channel for Capacitive PUF-Based Security Enclosures

Kathrin Garb, Marvin Xhemrishi, Ludwig Kürzinger, Christoph Frisch
Technical University of Munich, Munich, Germany

Conference on Cryptographic Hardware and Embedded Systems
Leuven, Belgium, September 21, 2022
Outline

Capacitive PUF-Based Security Enclosures

System Model

Wiretap Channel Implementation

Summary
Capacitive PUF-Based Security Enclosures
Capacitive PUF-Based Security Enclosures

Motivation

Hardware Security Modules (HSMs) require a physical boundary

Battery-backed enclosures
- Continuous power supply
- Reduced lifetime

---

\(^1\)ISO/IEC 24759, FIPS 140-3, BSI-CC-PP-0045
Capacitive PUF-Based Security Enclosures

Motivation

Hardware Security Modules (HSMs) require a physical boundary \(^1\)

Battery-backed enclosures \(^2\)
- Continuous power supply
- Reduced lifetime

Enclosures based on Physical Unclonable Functions (PUFs)
- A PUF is a fingerprint of an object formed by minuscule manufacturing variations
- No continuous power supply required

\(^1\)ISO/IEC 24759, FIPS 140-3, BSI-CC-PP-0045
Capacitive PUF-Based Security Enclosures

System Overview

- Meander structure with 32 overlapping electrodes $\Rightarrow$ 256 absolute capacitances
- PUF-response: 128 differential capacitances (different for each enclosure)$^3$
- Generation of key from PUF-response
- Protection against 300 $\mu$m drill diameters$^4$

---


Capacitive PUF-Based Security Enclosures

Tamper-Sensitive Error Correction

Reliably reproducible PUF-response ⇒ Error correction codes

• Correcting environmental effects

---

Capacitive PUF-Based Security Enclosures

Tamper-Sensitive Error Correction

Reliably reproducible PUF-response \implies Error correction codes

- Correcting environmental effects
- However: Correcting attack?

Capacitive PUF-Based Security Enclosures

Tamper-Sensitive Error Correction

Reliably reproducible PUF-response ⇒ Error correction codes

• Correcting environmental effects
• However: Correcting attack?
• Goal: Description through wiretap channel

---

Capacitive PUF-Based Security Enclosures

Tamper-Sensitive Error Correction

Reliably reproducible PUF-response $\Rightarrow$ Error correction codes

- Correcting environmental effects
- However: Correcting attack?
- **Goal:** Description through wiretap channel

Wiretap channel implementations for PUFs$^5$ $^6$ $^7$

- Binary silicon PUFs
- Unstable or biased PUF-bits

---


Capacitive PUF-Based Security Enclosures

Contributions

- System model
  - Modeling of thermal effects and drilling attacks
  - Consideration of post-processing
Capacitive PUF-Based Security Enclosures

Contributions

• System model
  • Modeling of thermal effects and drilling attacks
  • Consideration of post-processing

• Construction of wiretap channel via $q$-ary polar codes
  • Error correction of Higher Order Alphabet PUF
  • Code construction through Monte Carlo simulation
  • Determine security level of the code construction
  • Calculate entropy of the PUF-secret
System Model
System Model

Post Processing

• Differential capacitances with Gaussian distribution\(^8\)
• Normalization, quantization (\(q\)-ary alphabet)
• Quantized PUF-response ⇒ Input to key generation (Fuzzy Commitment)

System Model

Temperature Measurement

\[ [0, 10000] \cong [0 \text{ pF}, 100 \text{ pF}] \]

\[ [-10000, 10000] \cong [-134 \text{ fF}, 134 \text{ fF}] \]

---


Kathrin Garb (TUM) | IACR CHES 2022 | The Wiretap Channel for Capacitive PUF-Based Security Enclosures 8
System Model

Temperature

- Comparison of raw and normalized PUF-response
- Distribution mean changes
- Standard deviation reduced
- $\Delta \sigma = 207$ points (20°C to 60°C)
System Model

Drilling Attacks

- A 300 µm drill destroys two electrodes
- Normalization reduces large offsets
- The attack causes burst errors
System Model

Drilling Attacks

• Attack broadens the distribution
• Before normalization: $\Delta \sigma = 3295$ points
• After normalization: $\Delta \sigma = 787$ points > 207 points (thermal changes)
Wiretap Channel Implementation
The Wiretap Channel...
...for Capacitive PUF-Based Enclosures

- Introduced by A. D. Wyner\textsuperscript{10}
- Main channel: thermal effects $\hat{\epsilon}_t$, noise $\hat{\epsilon}_n \Rightarrow$ error probability $p_1$
- Second channel: additionally affected by attack $\hat{\epsilon}_a \Rightarrow$ error probability $p_2$

The Wiretap Channel

Code Construction

- $q$-ary polar codes ($n = 128$) with SC and SCL decoding
- Probability matrix $P(y|c)$ for 8, 16, 32 equiprobable intervals
- Code construction through Monte Carlo simulation
The Wiretap Channel

Results of Monte Carlo Simulation

<table>
<thead>
<tr>
<th>Decoder</th>
<th>q</th>
<th>FER</th>
<th>$H_{att}$</th>
<th>$H_{secret}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCD</td>
<td>8</td>
<td>$4.0 \times 10^{-6}$</td>
<td>100</td>
<td>306</td>
</tr>
<tr>
<td>SCL ($L = 8$)</td>
<td>8</td>
<td>$1.0 \times 10^{-6}$</td>
<td>100</td>
<td>306</td>
</tr>
<tr>
<td>SCD</td>
<td>32</td>
<td>$7.0 \times 10^{-6}$</td>
<td>57</td>
<td>275</td>
</tr>
<tr>
<td>SCL ($L = 8$)</td>
<td>32</td>
<td>$3.3 \times 10^{-6}$</td>
<td>57</td>
<td>275</td>
</tr>
</tbody>
</table>

- Complexity for an attacker $H_{att} = - \sum_{i}^{ns} p_{s,i} \log_2(p_{s,i})$
  with $p_{s,i}$ the symbol error rate after an attack
- Achievable security level $2^{H_{att}}$
- Entropy of the PUF-secret $H_{secret}$
Summary
Summary

- System model for environmental changes and attack effects
Summary

- System model for environmental changes and attack effects
- Construction of a wiretap channel for the capacitive PUF-based enclosure from $q$-ary polar codes

$\Rightarrow$ Relevance for other PUFs

$\Rightarrow$ Distinguish different effects through wiretap coding
Summary

• System model for environmental changes and attack effects
• Construction of a wiretap channel for the capacitive PUF-based enclosure from $q$-ary polar codes
• Monte Carlo simulation
  • Physical layer security of 100 bits ($q = 8$)
  • 306-bits of entropy for PUF-secret ($q = 8$)
Summary

- System model for environmental changes and attack effects
- Construction of a wiretap channel for the capacitive PUF-based enclosure from $q$-ary polar codes
- Monte Carlo simulation
  - Physical layer security of 100 bits ($q = 8$)
  - 306-bits of entropy for PUF-secret ($q = 8$)

⇒ Relevance for other PUFs
⇒ Distinguish different effects through wiretap coding
Thank you for your attention!
The Wiretap Channel

Results

- Per-symbol error probability $d$
- $d$ determines the number of symbols $n_s$ ⇒ trade-off between security and reliability

<table>
<thead>
<tr>
<th>$q$</th>
<th>Without $W''$</th>
<th>With $W''$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$d$</td>
<td>$n_s$</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.0500</td>
<td>91</td>
<td>11</td>
</tr>
<tr>
<td>0.0100</td>
<td>85</td>
<td>11</td>
</tr>
<tr>
<td>0.0050</td>
<td>82</td>
<td>11</td>
</tr>
<tr>
<td>0.0010</td>
<td>73</td>
<td>11</td>
</tr>
<tr>
<td>0.0005</td>
<td>71</td>
<td>11</td>
</tr>
<tr>
<td>0.0001</td>
<td>65</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10^{-6}</td>
<td>56</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.0500</td>
<td>80</td>
<td>11</td>
</tr>
<tr>
<td>0.0100</td>
<td>75</td>
<td>11</td>
</tr>
<tr>
<td>0.0050</td>
<td>72</td>
<td>11</td>
</tr>
<tr>
<td>0.0010</td>
<td>68</td>
<td>11</td>
</tr>
<tr>
<td>0.0005</td>
<td>66</td>
<td>11</td>
</tr>
<tr>
<td>0.0001</td>
<td>62</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10^{-6}</td>
<td>55</td>
</tr>
<tr>
<td></td>
<td>&lt; 10^{-6}</td>
<td>56</td>
</tr>
</tbody>
</table>
The Wiretap Channel

Results of Monte Carlo Simulation

<table>
<thead>
<tr>
<th>Decoder</th>
<th>$q$</th>
<th>FER</th>
<th>$n_s$</th>
<th>$n_f$</th>
<th>$H_{\text{att}}$</th>
<th>$H_{\text{secret}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCD</td>
<td>8</td>
<td>$4.0 \times 10^{-6}$</td>
<td>102</td>
<td>22</td>
<td>100</td>
<td>306</td>
</tr>
<tr>
<td>SCL ($L = 8$)</td>
<td>8</td>
<td>$1.0 \times 10^{-6}$</td>
<td>102</td>
<td>22</td>
<td>100</td>
<td>306</td>
</tr>
<tr>
<td>SCD</td>
<td>32</td>
<td>$7.0 \times 10^{-6}$</td>
<td>55</td>
<td>11</td>
<td>57</td>
<td>275</td>
</tr>
<tr>
<td>SCL ($L = 8$)</td>
<td>32</td>
<td>$3.3 \times 10^{-6}$</td>
<td>55</td>
<td>11</td>
<td>57</td>
<td>275</td>
</tr>
</tbody>
</table>

• Complexity for an attacker $H_{\text{att}} = - \sum_{i}^{n_s} p_{s,i} \log_2(p_{s,i})$
  with $p_{s,i}$ the symbol error rate after an attack

• Achievable security level $2^{H_{\text{att}}}$

• $n_s = k$ symbols are reliably reproduced with entropy $H_{\text{secret}} = n_s \log_2(q)$ bits
System Model

Key Generation via Fuzzy Commitment

- Key generated from TRNG \(\Rightarrow\) Second enrollment possible after transport\(^{11}\)
- Additional randomness is introduced \(\Rightarrow\) Wiretap channel scenario

System Model

Quantization

- Gray encoding: Binary number of $\log_2(m)$ bits
- Binary model not sufficient $\Rightarrow q$-ary alphabet
- $q$-ary model $\Rightarrow$ increased sensitivity towards tampering