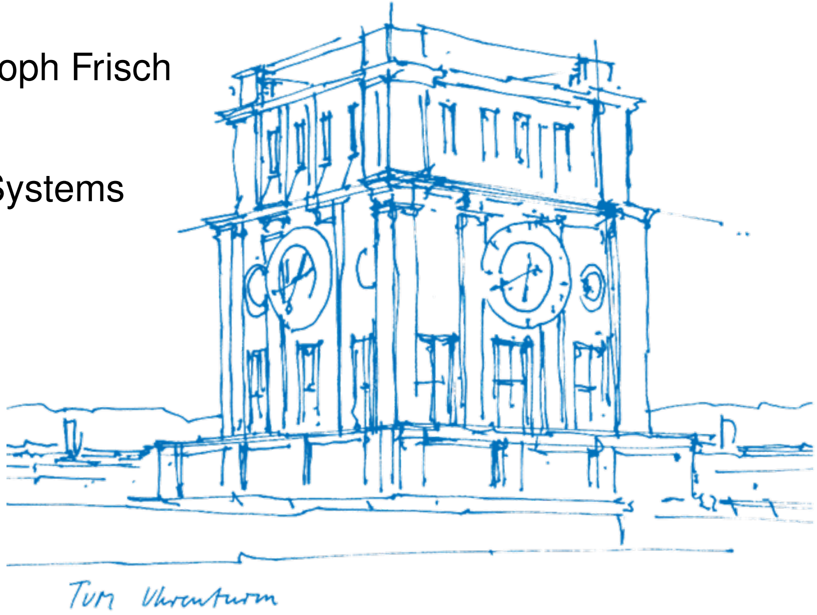
The Wiretap Channel for Capacitive PUF-Based Security Enclosures

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

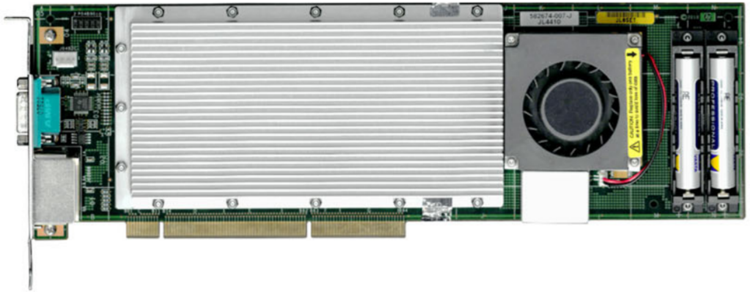
Capacitive PUF-Based Security Enclosures

Motivation

Hardware Security Modules (HSMs) require a physical boundary [1]

Battery-backed enclosures [2]

- Continuous power supply
- Reduced lifetime



[1] ISO/IEC 24759, FIPS 140-3, BSI-CC-PP-0045

[2] J. Obermaier, V. Immler. J Hardw Syst Secur, 2018.

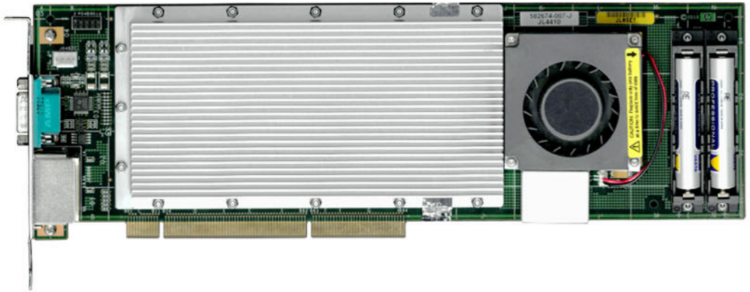
Capacitive PUF-Based Security Enclosures

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)

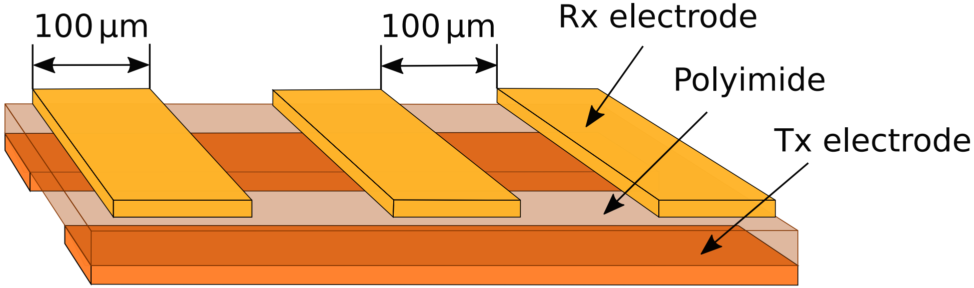
- A PUF is a fingerprint of an object formed by minuscule manufacturing variations
- No continuous power supply required

[1] ISO/IEC 24759, FIPS 140-3, BSI-CC-PP-0045

[2] J. Obermaier, V. Immler. J Hardw Syst Secur, 2018.

Capacitive PUF-Based Security Enclosures

System Overview



- Meander structure with 32 overlapping electrodes ⇒ 256 absolute capacitances
- PUF-response: 128 differential capacitances (different for each enclosure)[3]
- Generation of key from PUF-response
- Protection against 300 µm drill diameters[4]

[3] V. Immler, J. Obermaier, K. K. Ng, F. X. Ke, J. Y. Lee, Y. P. Lim, W. K. Oh, K. H. Wee, and G. Sigl. CHES, pages 51-96, 2019.
[4] K. Garb, M. Schink, M. Hiller, and J. Obermaier. IEEE PAINE, pages 1-8, 2021.

Capacitive PUF-Based Security Enclosures

Tamper-Senstive Error Correction

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

- Correcting environmental effects

[5] M. Hiller and A. G. Önalan. CHES, pages 601-619. Springer, 2017.
[6] Y. Bai and Z. Yan. IEEE SiPS, pages 254-259, 2019.
[7] Y. Bai and Z. Yan. Journal of Electronic Testing, Vol. 37, June 2021.

Capacitive PUF-Based Security Enclosures

Tamper-Senstive Error Correction

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

- Correcting environmental effects
- <u>However:</u> Correcting attack?

[5] M. Hiller and A. G. Önalan. CHES, pages 601-619. Springer, 2017.
[6] Y. Bai and Z. Yan. IEEE SiPS, pages 254-259, 2019.
[7] Y. Bai and Z. Yan. Journal of Electronic Testing, Vol. 37, June 2021.

Capacitive PUF-Based Security Enclosures

Tamper-Senstive Error Correction

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

- Correcting environmental effects
- <u>However:</u> Correcting attack?
- **Goal:** Description through wiretap channel

---

[5] M. Hiller and A. G. Önalan. CHES, pages 601-619. Springer, 2017.
[6] Y. Bai and Z. Yan. IEEE SiPS, pages 254-259, 2019.
[7] Y. Bai and Z. Yan. Journal of Electronic Testing, Vol. 37, June 2021.

Capacitive PUF-Based Security Enclosures

Tamper-Senstive Error Correction

Reliably reproducible PUF-response ⇒ Error correction codes

- Correcting environmental effects
- <u>However:</u> Correcting attack?
- **Goal:** Description through wiretap channel

Wiretap channel implementations for PUFs[5] [6] [7]

- Binary silicon PUFs
- Unstable or biased PUF-bits

[5] M. Hiller and A. G. Önalan. CHES, pages 601-619. Springer, 2017.
[6] Y. Bai and Z. Yan. IEEE SiPS, pages 254-259, 2019.
[7] Y. Bai and Z. Yan. Journal of Electronic Testing, Vol. 37, June 2021.

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

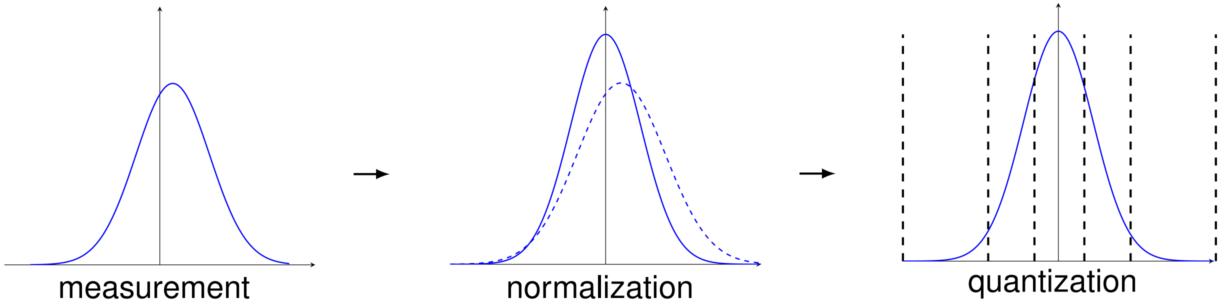
- System model
    - Modeling of thermal effects and drilling attacks
    - Consideration of post-processing

- 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

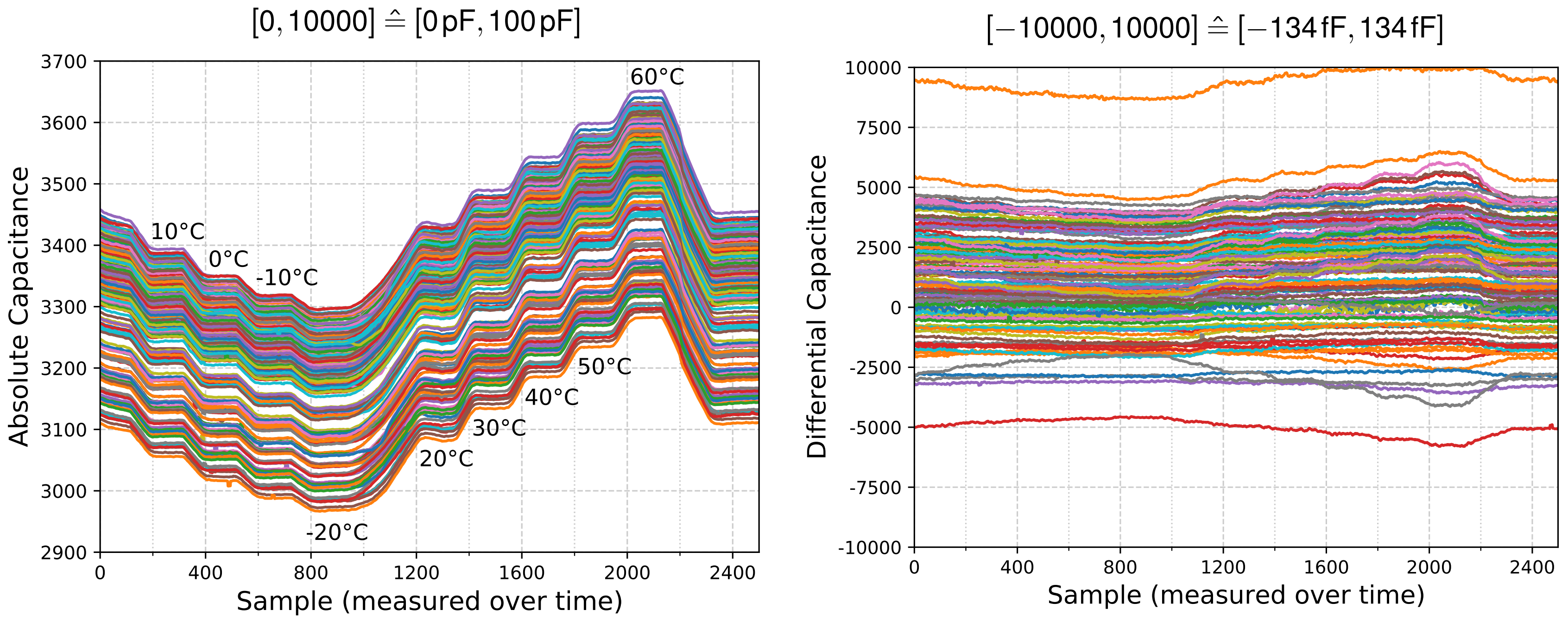


- Differential capacitances with Gaussian distribution[8]
- Normalization, quantization ($q-$ary alphabet)
- Quantized PUF-response $\Rightarrow$ Input to key generation (Fuzzy Commitment)

[8] V. Immler, J. Obermaier, K. K. Ng, F. X. Ke, J. Y. Lee, Y. P. Lim, W. K. Oh, K. H. Wee, and G. Sigl. CHES, pages 51-96, 2019.

System Model

Temperature Measurement[9]

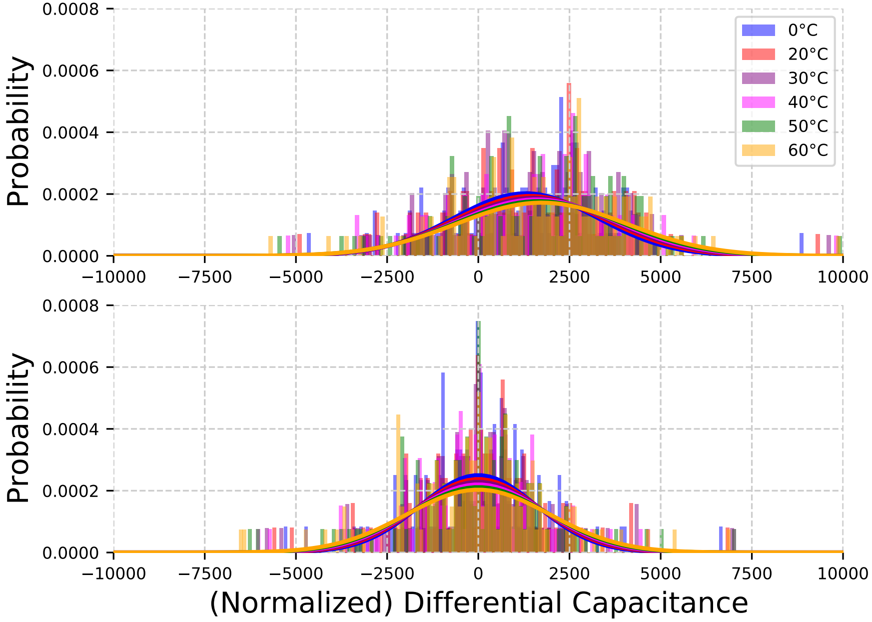


[9] V. Immler, J. Obermaier, K. K. Ng, F. X. Ke, J. Y. Lee, Y. P. Lim, W. K. Oh, K. H. Wee, and G. Sigl. CHES, pages 51-96, 2019.

System Model

Temperature

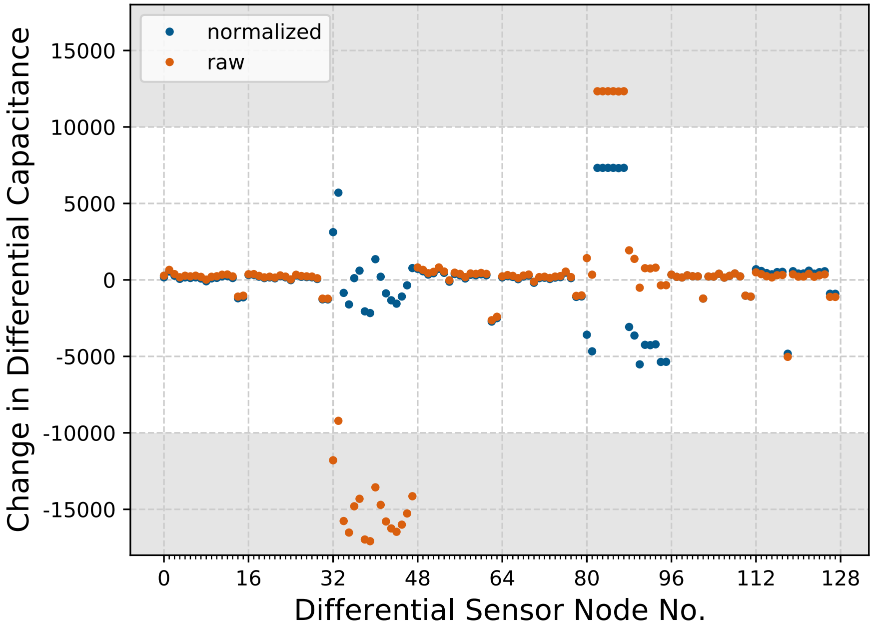
- Comparison of raw and normalized PUF-response
- Distribution mean changes
- Standard deviation reduced
- $\Delta\sigma = 207$ points (20 °C to 60 °C)



System Model

Drilling Attacks

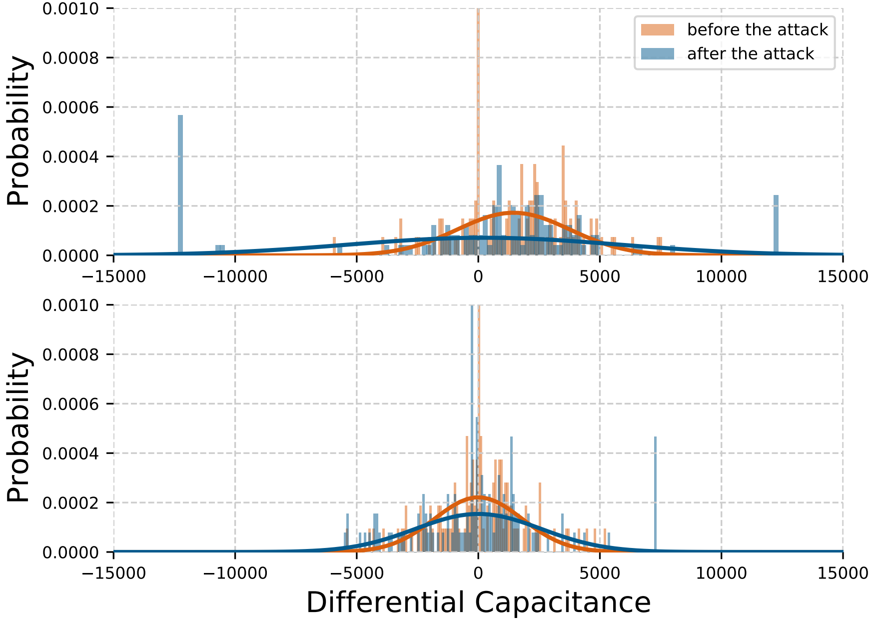
- A 300 µm drill destroys two electrodes
- Normalization reduces large offsets
- The attack causes burst errors



System Model

Drilling Attacks

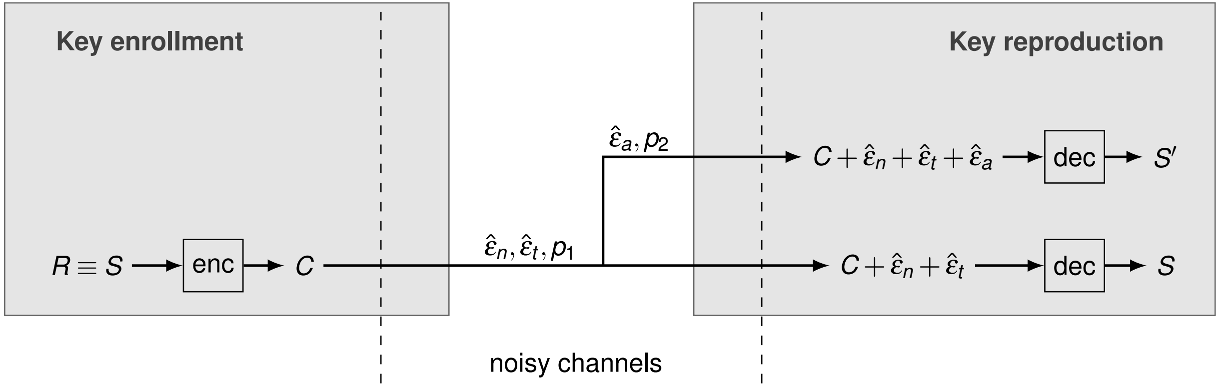
- Attack broadens the distribution
- Before normalization: $\Delta\sigma = 3295$ points
- After normalization: $\Delta\sigma = 787$ points > 207 points (thermal changes)



Wiretap Channel Implementation

The Wiretap Channel...

...for Capacitive PUF-Based Enclosures



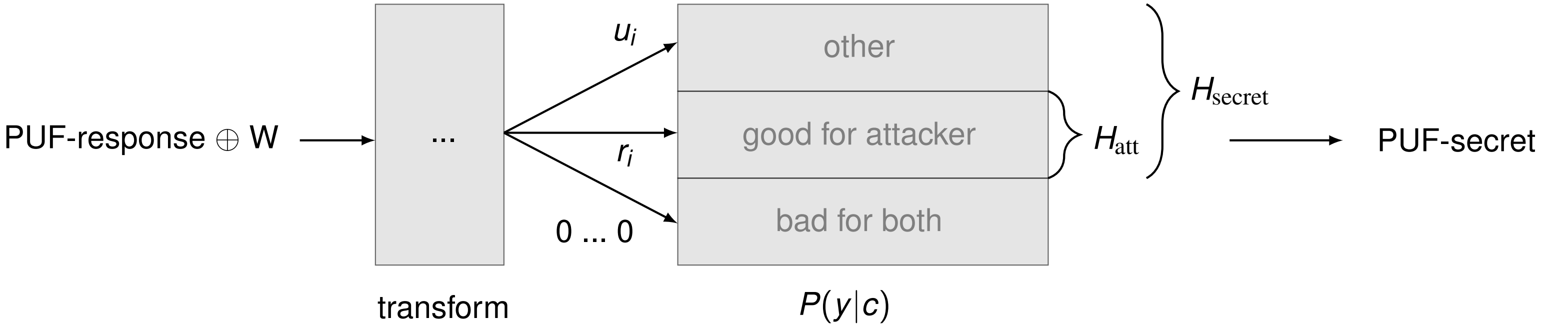
- Introduced by A. D. Wyner[10]
- Main channel: thermal effects $\hat{\varepsilon}_t$, noise $\hat{\varepsilon}_n \Rightarrow$ error probability p_1
- Second channel: additionally affected by attack $\hat{\varepsilon}_a \Rightarrow$ error probability p_2

[10] A. D. Wyner. The wire-tap channel. The Bell System Technical Journal, 54(8):1355–1387, 1975.

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

Decoder	q	FER	$\mathbf{H}_{\text{att}}$	$\mathbf{H}_{\text{secret}}$
SCD	8	4.0×10^{-6}	**100**	**306**
SCL ($L = 8$)	8	1.0×10^{-6}	**100**	**306**
SCD	32	7.0×10^{-6}	**57**	**275**
SCL ($L = 8$)	32	3.3×10^{-6}	**57**	**275**

- 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 $2^{H_{\text{att}}}$
- 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

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 ($q = 8$)

$\Rightarrow$ Relevance for other PUFs

$\Rightarrow$ 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 $n_s \Rightarrow$ trade-off between security and reliability

q	Without W'					With W'				
	d	n_s	n_f	H_{att}	H_{secret}	d	n_s	n_f	H_{att}	H_{secret}
8	0.0500	91	11	113.5	273	0.0500	123	22	163.0	369
	0.0100	85	11	95.6	255	0.0100	121	22	157.9	363
	0.0050	82	11	86.8	246	0.0050	120	22	154.9	360
	0.0010	73	11	60.8	219	0.0010	119	22	151.9	357
	0.0005	71	11	55.6	213	0.0005	117	22	145.9	351
	0.0001	65	11	40.2	195	0.0001	112	22	130.9	336
	-					10^{-5}	106	22	112.0	318
	10^{-6}	56	11	22.1	168	**10^{-6}**	**102**	**22**	**100.3**	**306**
	-					$< 10^{-6}$	101	22	98.0	303
32	0.0500	80	11	168.7	400	0.0500	86	15	181.0	430
	0.0100	75	11	143.0	375	0.0100	78	15	141.4	390
	0.0050	72	11	129.4	360	0.0050	76	15	131.7	380
	0.0010	68	11	111.4	340	0.0010	73	15	116.9	365
	0.0005	66	11	102.5	330	0.0005	72	15	112.4	360
	0.0001	62	11	89.1	310	0.0001	69	15	98.9	345
	-					10^{-5}	62	15	74.0	310
	10^{-6}	**55**	**11**	**57.3**	**275**	10^{-6}	58	15	58.9	290
	-					$< 10^{-6}$	56	15	49.9	280

The Wiretap Channel

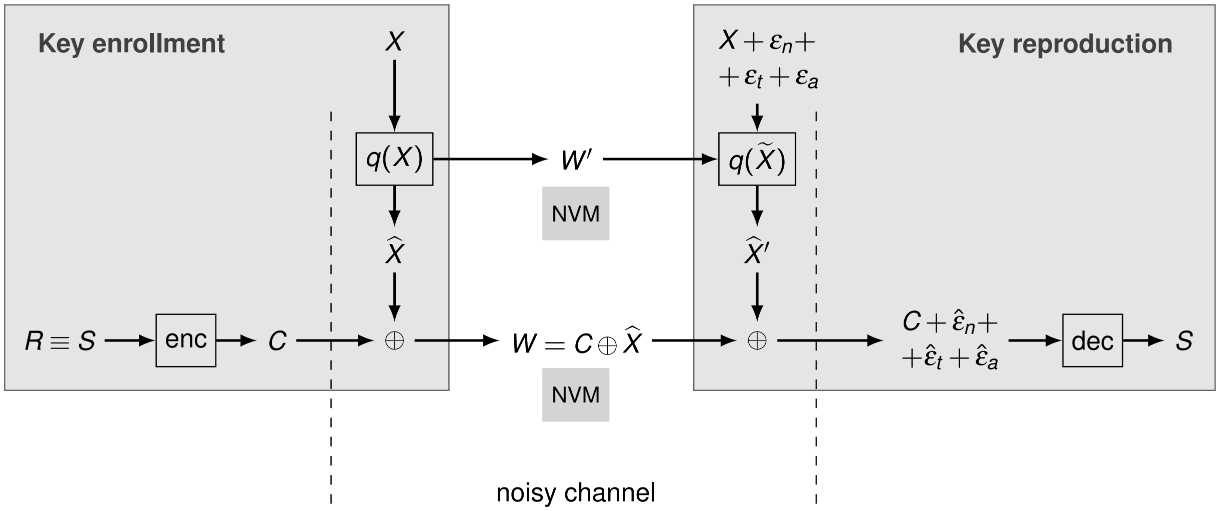
Results of Monte Carlo Simulation

Decoder	q	FER	n_s	n_f	$\mathbf{H}_\text{att}$	$\mathbf{H}_\text{secret}$
SCD	8	4.0×10^{-6}	102	22	**100**	**306**
SCL ($L = 8$)	8	1.0×10^{-6}	102	22	**100**	**306**
SCD	32	7.0×10^{-6}	55	11	**57**	**275**
SCL ($L = 8$)	32	3.3×10^{-6}	55	11	**57**	**275**

- 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_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 ⇒ Second enrollment possible after transport[11]
- Additional randomness is introduced ⇒ Wiretap channel scenario

[11] K. Garb, J. Obermaier, E. Ferres, and M. König. 18th International Conference on Privacy, Security and Trust. 2021.

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