SPONSORED BY THE
Federal Ministry of Education and Research

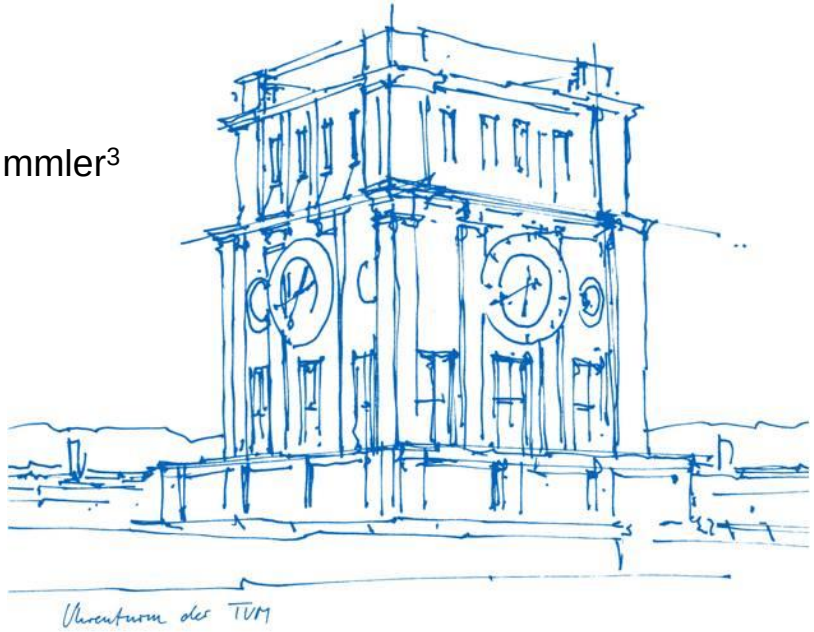
Spatial Context Tree Weighting for Physical Unclonable Functions

Michael Pehl[1], Tobias Tretschok[1], Daniel Becker[2], Vincent Immler[3]

[1] Technical University of Munich

[2] Ruhr-Universität Bochum

[3] Fraunhofer Institute for Applied and Integrated Security



Agenda

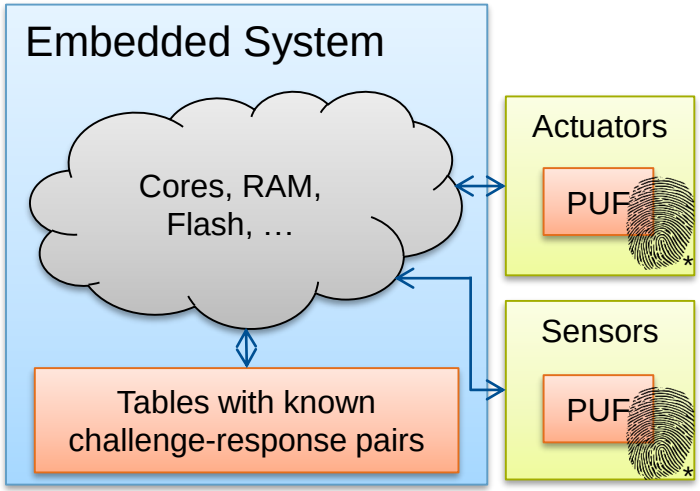
- Entropy Estimation of Physical Unclonable Functions:

  Motivation and State of the Art

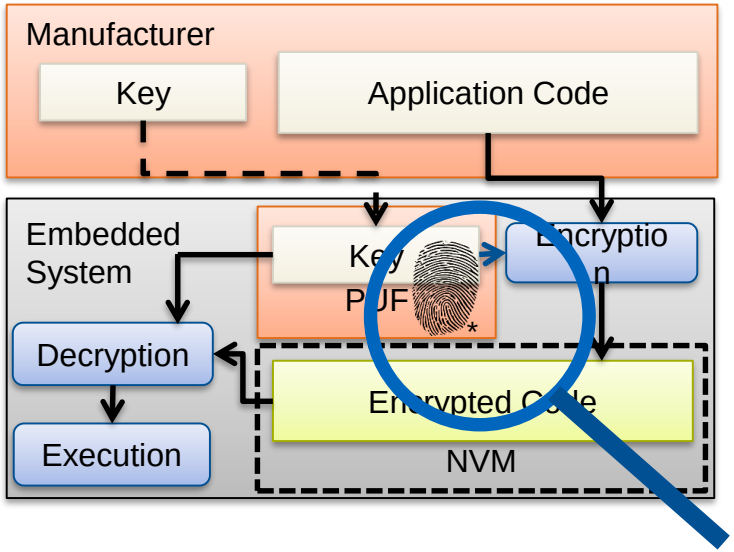
- Spatial Context Tree Weighting
- Practical Results of Entropy Estimation
- Conclusion

Physical Unclonable Functions (PUFs)

PUF for Authentication/Identification



PUF for Key-Storage



- PUFs provide a device unique secret
- The security level strongly depends on the PUF‘s quality

** The Photographer (Own work); licensed under CC BY-SA-3.0*

State of the Art in Weak PUF Evaluation

Statistical Metrics:

- Maiti et al., *A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions:* Bit-Alias, Uniformity, Uniqueness …
- Wilde et al., *On the Confidence in Bit-Alias Measurement of Physical Unclonable Functions:* Confidence intervals on Bit-Alias.
- Hori et al., *Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs*: Randomness, Diffuseness, Uniqueness …
- Wilde et al., *Statistic-based security analysis of ring oscillator PUFs:* PCA.
- Wilde et al., *Spatial Correlation Analysis on Physical Unclonable Functions:* Statistical analysis of spatial effects.

→ Provide various insides in PUFs, but hard to interpret.

State of the Art in Weak PUF Evaluation

How hard is it to guess the key? → Entropy Metrics:

- Ignatenko et al., *Estimating the Secrecy-Rate of Physical Unclonable Functions with the Context-Tree Weighting Method:* First to apply context tree weighting to PUFs, spatial dependencies not systematically analyzed.
- Pehl et al., *Efficient Evaluation of Physical Unclonable Functions Using Entropy Measures:* Dependency of entropy and potential defects analyzed, no spatial dependencies considered.
- Wilde et al., *Efficient Bound for Conditional Min-Entropy of Physical Unclonable Functions Beyond IID:* Estimation of entropy remaining in a key, no spatial dependencies considered

→ Our goal: Consider spatial dependencies to improve entropy bounds for array like PUFs

Agenda

- Entropy Estimation of Physical Unclonable Functions:

  Motivation and State of the Art

- Spatial Context Tree Weighting
- Practical Results of Entropy Estimation
- Conclusion

Context Tree Weighting (CTW)*

Given: Sequence of symbols $x = x_0, x_1, \dots, x_N$

Assumption: current symbol depends only on last D symbols

Algorithm:

- Model source as a tree source with depth D
- Approximate probability of sequences to appear
- Probability of the root node (coding probability P_c) is a measure for entropy

Entropy estimation for PUFs:

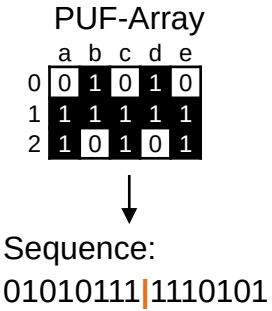
- Entropy in the sequence (PUF): $H_{PUF} \leq -\frac{\log_2 P_c}{N-D}$

* Willems et al. *Context Tree Weighting : A Sequential Universal Source Coding Procedure for FSMX Sources*

Context Tree Weighting (CTW)*

Given: Sequence of symbols $x = x_0 x_1, \dots, x_N$

Assumption: current symbol depends only on last D symbols → **Let $D = 8$**



Algorithm:

- Model source as a tree source with depth D
- Approximate probability of sequences to appear
- Probability of the root node (coding probability P_c) is a measure for entropy

Entropy estimation for PUFs:

- Entropy in the sequence (PUF): $H_{PUF} \leq -\frac{\log_2 P_c}{N-D}$

* Willems et al. *Context Tree Weighting : A Sequential Universal Source Coding Procedure for FSMX Sources*

Context Tree Weighting (CTW)*

Given: Sequence of symbols $x = x_0 x_1, \dots, x_N$

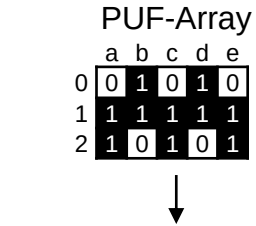
Assumption: current symbol depends only on last D symbols → **Let $D = 8$**

Algorithm:

- Model source as a tree source with depth D
- Approximate probability of sequences to appear
- Probability of the root node (coding probability P_c) is a measure for entropy

Entropy estimation for PUFs:

- Entropy in the sequence (PUF): $H_{PUF} \leq -\frac{\log_2 P_c}{N-D}$



Context	Following Zeros/Ones
01010111	0/1

* Willems et al. *Context Tree Weighting : A Sequential Universal Source Coding Procedure for FSMX Sources*

Context Tree Weighting (CTW)*

Given: Sequence of symbols $x = x_0 x_1, \dots, x_N$

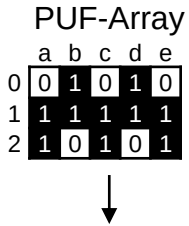
Assumption: current symbol depends only on last D symbols → **Let $D = 8$**

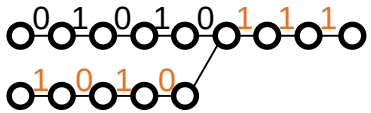
Algorithm:

- Model source as a tree source with depth D
- Approximate probability of sequences to appear
- Probability of the root node (coding probability P_c) is a measure for entropy

Entropy estimation for PUFs:

- Entropy in the sequence (PUF): $H_{PUF} \leq -\frac{\log_2 P_c}{N-D}$



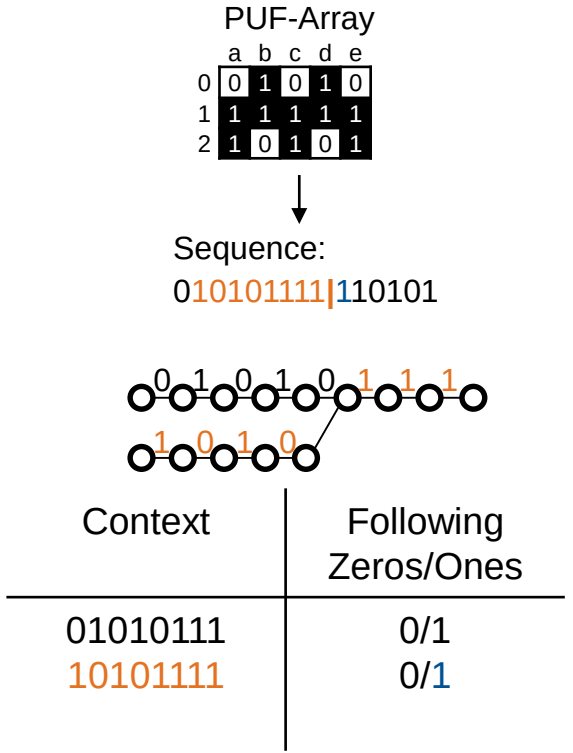


Context	Following Zeros/Ones
01010111	0/1
10101111	0/1

* Willems et al. *Context Tree Weighting : A Sequential Universal Source Coding Procedure for FSMX Sources*

Entropy Estimation of PUFs with CTW

- CTW provides an upper bound for entropy
- No spatial ordering considered
  → sequences w/o physical meaning used for entropy estimation
- Dependencies are considered within the last D elements
  → likely dependent responses might be not in the same sequence



From CTW to Spatial Context Tree Weighting (SCTW)

Classical CTW (CCTW)

- Considers only dependencies in last D elements
  → *Relevant* PUF responses shall appear in the context

PUFs

- Are frequently arranged in arrays
- Are rather correlated when spatially close
  → Responses of spatially close PUFs are *relevant*.

⇒ Re-Interpretation of context:
CCTW: Context of conditioned symbol = last symbols in sequence.
SCTW: Context of conditioned symbol = neighboring bits.
We have proven: SCTW still approximates entropy

CCTW-Context

	a	b	c	d	e
0	0	1	0	1	0
1	1	1	1	1	1
2	1	0	1	0	1

SCTW-Context

	a	b	c	d	e
0	0	1	0	1	0
1	1	1	1	1	1
2	1	0	1	0	1

Considered CTW-Variants

- All variants: consideration of higher order alphabet responses
- Classical CTW (CCTW):
  - Responses concatenated row-wise
- Spatial CTW (SCTW):
  - Considers neighboring bits
  - Well suited to detect spatial defects
- Forward CTW (FCTW)
  - Similar to SCTW
  - Less balanced: some bits only seldom in context
- Horizontal CTW (HCTW) / Vertical CTW (VCTW)
  - Well suited to find correlations in rows/columns
  - Help to identify specific defects

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
0										7			8	7	6
1	5	4	3	2	1	X				5					
2										3					
3		8	1	5						1					
4		4	X	2						X		X	1	3	
5		7	3	6						2		2	4	6	
6										4		5	7	8	
7	7	5	3	1	X	2	4	6	8	6					
8										8					

Agenda

- Entropy Estimation of Physical Unclonable Functions:

  Motivation and State of the Art

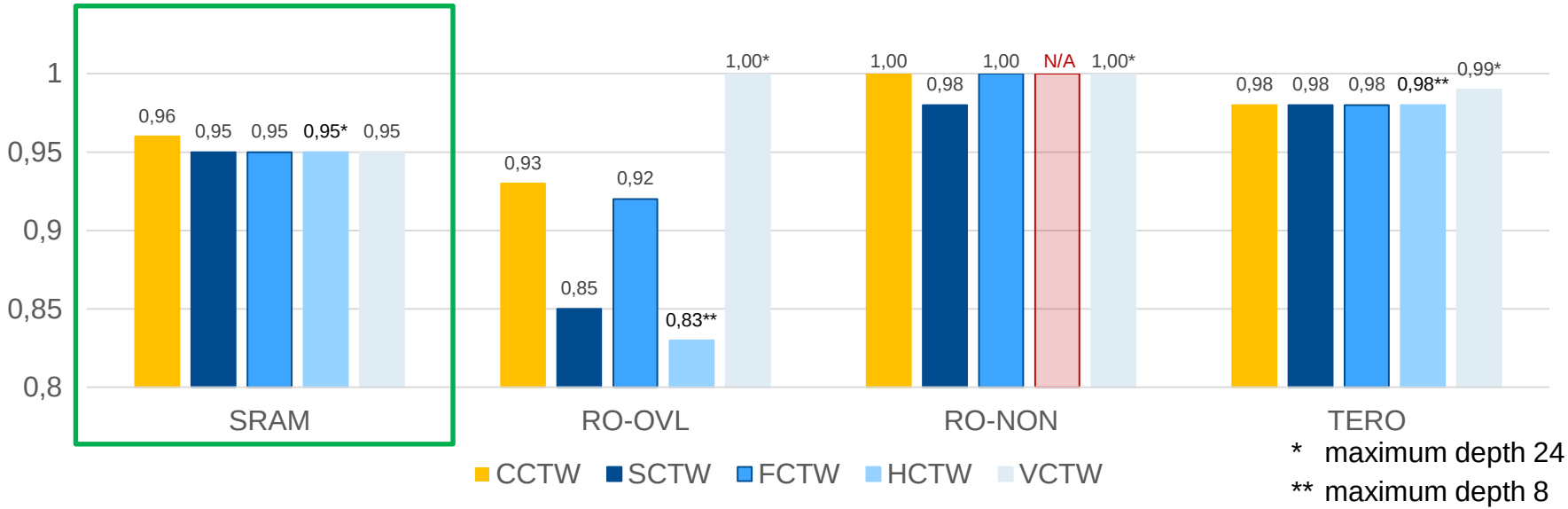
- Spatial Context Tree Weighting
- Practical Results of Entropy Estimation
- Conclusion

Analyzed Data

5 different PUF designs:

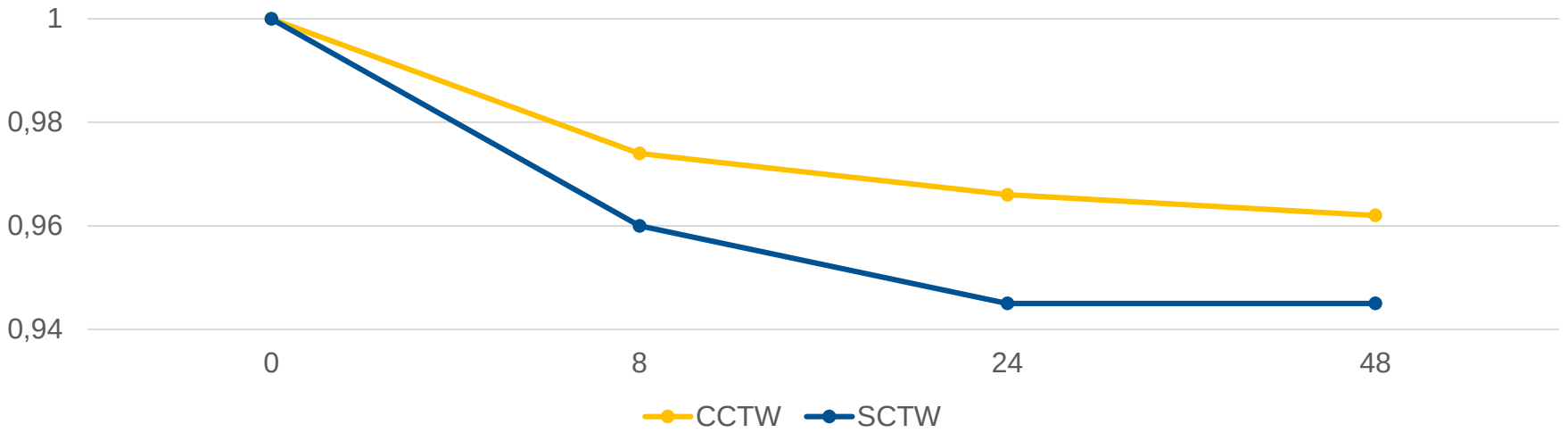
- SRAM (cf. Wilde, *Large Scale Characterization of SRAM on Infineon XMC Microcontrollers As PUF*):
  - Arrays of 32X40960 SRAM cells from 144 Microcontrollers (actual layout unknown)
- RO-OVL (cf. Maiti et al., *A Large Scale Characterization of RO-PUF*):
  - Arrays of 32X15 response bits derived from arrays of 32X16 ROs on 193 FPGAs
- RO-NON (cf. Maiti et al., *A Large Scale Characterization of RO-PUF*):
  - Arrays of 32X8 response bits derived from arrays of 32X16 ROs on 193 FPGAs
- TERO (cf. Wild et al., *A fair and comprehensive large-scale analysis of oscillation-based PUFs for FPGA*):
  - Arrays of 16X40 response bits derived from 16X80 TERO cells on 100 FPGAs
- Tamper-Evident PUF (cf. Immler et al. Secure Physical Enclosures from Covers with Tamper-Resistance):
  - Arrays of 8X16 capacitances each providing a 5-bit response symbol

Estimated Entropy for Different Weak PUFs (Tree Depth 48)



SCTW improves estimate in all experiments

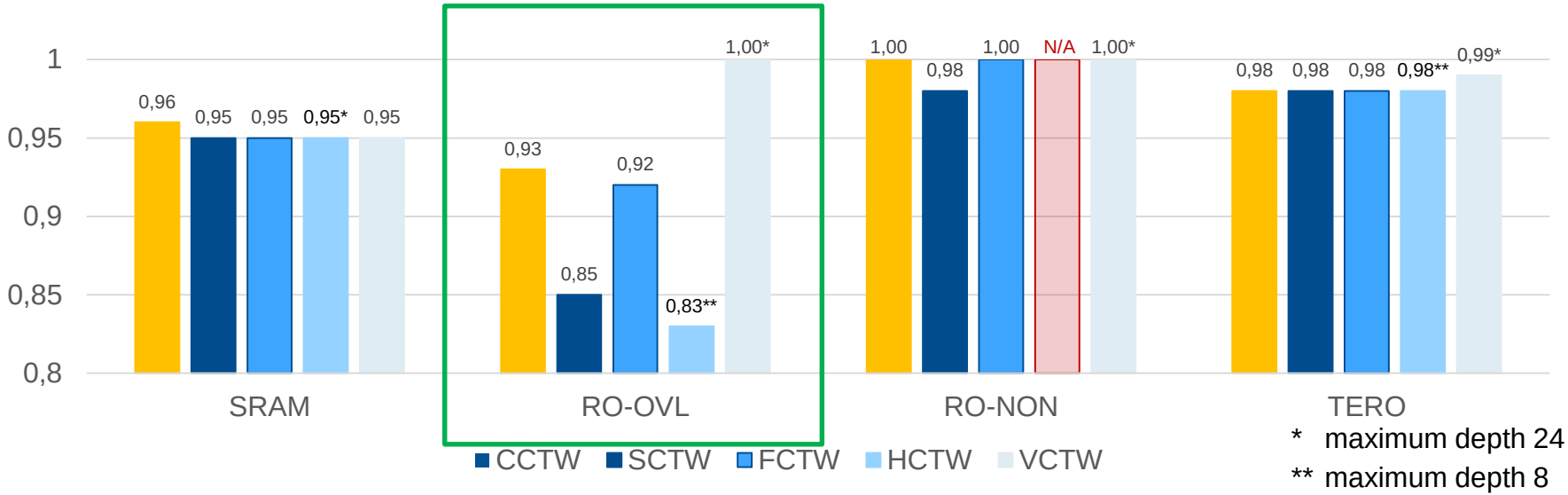
Entropy over Tree Depth: CCTW vs SCTW



SCTW covers important dependencies early

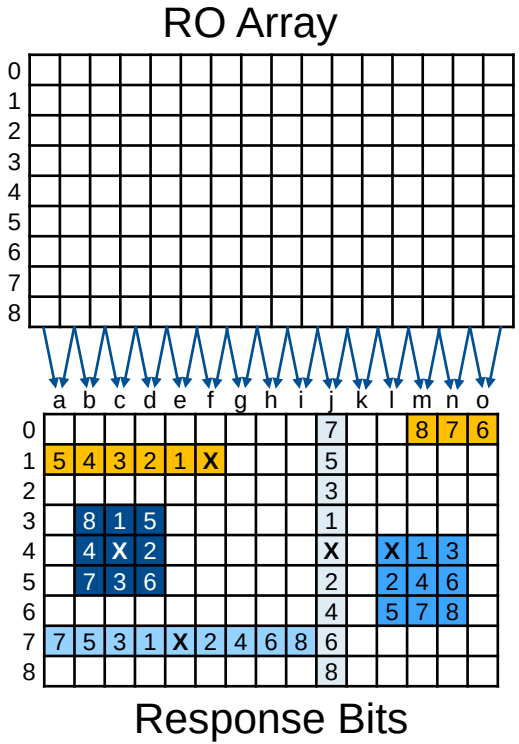
→ Better approximation with lower tree depth possible

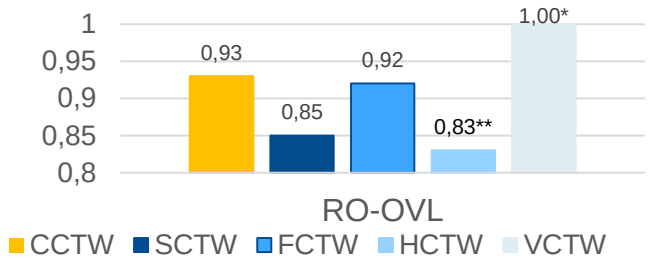
Estimated Entropy for Different Weak PUFs (Tree Depth 48)



SCTW improves estimate in all experiments

Estimated Entropy for Different Weak PUFs (Tree Depth 48)

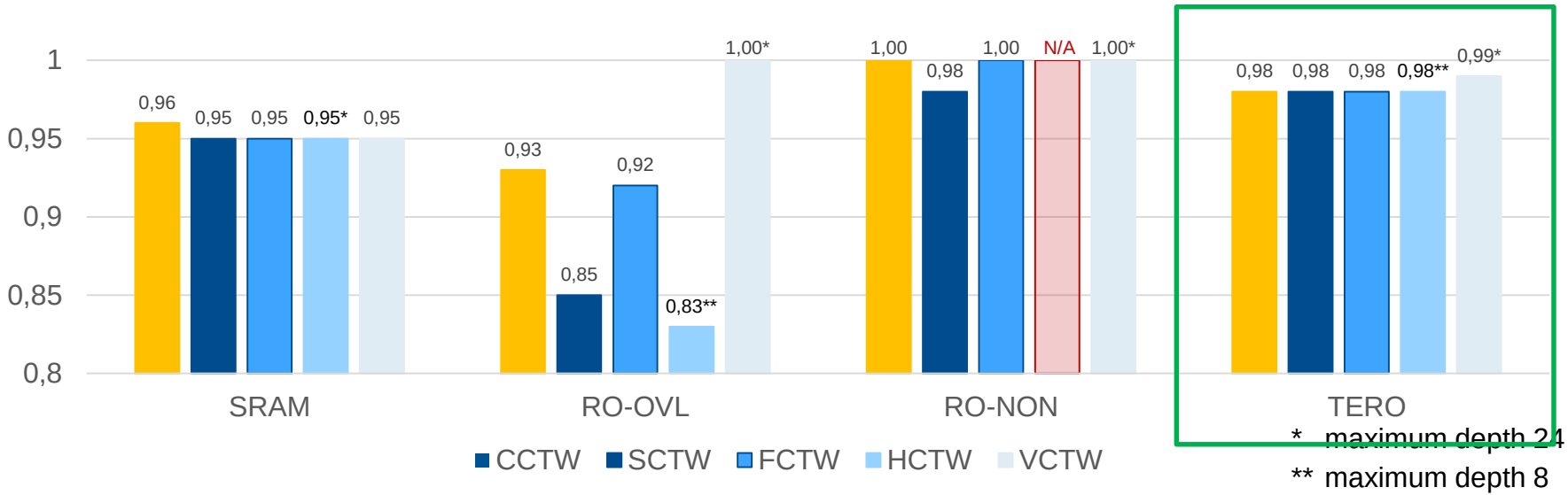




Frequencies compared in overlapping manner

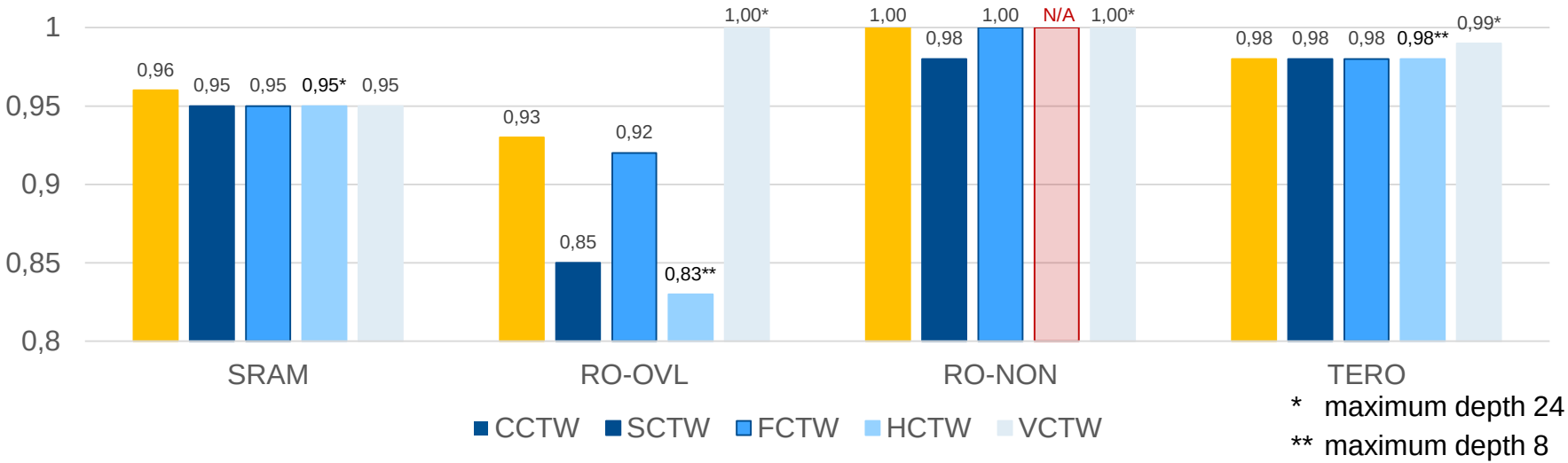
- → Correlation of bits in lines
- → CCTW: Estimate over line breaks
- → SCTW: Spatial dependencies in all directions
- → FCTW: Similar to SCTW but less well balanced
- → HCTW: Considers here most of the relevant dependencies with smallest depth
- → VCTW: Does not consider relevant dependencies

Estimated Entropy for Different Weak PUFs (Tree Depth 48)



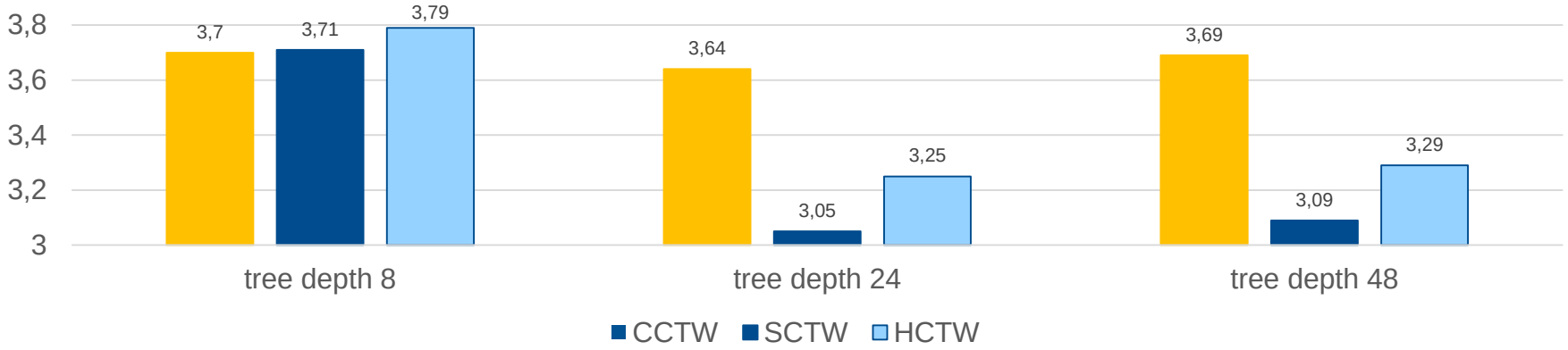
CCTW and SCTW result in same entropy → likely pure bias and no spatial defects

Estimated Entropy for Different Weak PUFs (Tree Depth 48)



- In general CCTW provides best estimate w/o pre knowledge
- Other context shapes: insights to possible design problems

Higher Order Alphabet PUF



- Target of analysis: tamper-evident PUF with 5 bit responses per position
- Significant improve of SCTW over CCTW
- Slide increase from dree depth 24 to 48 caused by numeric

Conclusion

We provided

- Extension of CTW to SCTW and further spatial variants

Benefits:

- Improved entropy bound through consideration of spatial effects.
- Application of different spatial variants reveals possible design issues.

Results:

- Analysis of 5 different PUF implementations
- Improved estimate of entropy (up to 16% for higher-order alphabet PUF)
- Improved bound given same tree depth (i.e., same computational effort)

Contact and Acknowledgement

Dr.-Ing. Michael Pehl
Technical University of Munich
Department of Electrical and Computer Engineering
Chair of Security in Information Technology
Arcisstr. 21, 80333 Munich, Germany
Email: m.pehl@tum.de

This work was partly funded by the German Federal Ministry for Education and Research through the project SecForCARs grant no. 16KIS0795