Towards the FPGA Platform Integration of Carbon-Nanotubes in Physical Unclonable Functions

Martin Schmid[1,*], Simon Böttger[2,3], Martin Ernst[2,3], Martin Hartmann[2,3], Sascha Hermann[2,3,4], Elif Bilge Kavun[5,6] and Stefan Katzenbeisser[1]

[1]*Faculty of Computer Science and Mathematics, University of Passau, Passau, Germany*
[2]*Center for Micro and Nano Technologies, Chemnitz University of Technology, Chemnitz, Germany*
[3]*Center for Materials, Architectures and Integration of Nanomembranes, Chemnitz University of Technology, Chemnitz, Germany*
[4]*Fraunhofer Institute of Electric Nano Systems, Chemnitz University of Technology, Chemnitz, Germany*
[5]*Barkhausen Institut, Dresden, Germany*
[6]*Institute of Systems Architecture, Dresden University of Technology, Dresden, Germany*

Abstract

Physical Unclonable Functions (PUFs) have emerged as a suitable implementation of hardware-based trust anchors, enabling secure key storage, device authentication, and software protection. Continuing research and developments have led to elevated technology readiness and highlight the potential of carbon nanotube field-effect transistors (CNTFETs) as the foundation for next-generation PUF architectures due to their high entropy, robustness, and thermal stability. In this work, we investigate 12×12 crossbar arrays composed of CNTFETs fabricated by scalable wafer-level manufacturing. We describe the measurement setup used to characterize the transistors and present the resulting electrical data. We analyze the impact of parasitic currents introduced by the interconnection of transistors' terminals, assessing their influence on the stability and reliability of the PUF response. Finally, we outline the design considerations and implementation constraints for interfacing the CNTFET matrix with an FPGA for digital readout, including an analysis of potential vulnerabilities introduced through this integration.

Keywords

Carbon-Nanotubes, Physical Unclonable Function, Field-Programmable Gate Array, Security Analysis

1. Introduction

Cyber-physical systems are increasingly deployed in safety-critical domains, including autonomous transportation, industrial automation, and critical infrastructure control. The security of such systems fundamentally relies on trust anchors that can authenticate devices [1], protect cryptographic keys [2], and detect unauthorized modifications [3]. Physical unclonable functions (PUFs) exploit stochastic assembly structure with controllable density to derive device-unique responses without storing secrets in non-volatile memory. Conventional CMOS-based PUFs, such as SRAM, Arbiter, and Ring Oscillator PUFs, have been widely studied. However, they often exhibit sensitivity to temperature and voltage variations and are susceptible to aging effects.

Emerging nanomaterials provide new opportunities to overcome these limitations. Among them, carbon nanotube field-effect transistors (CNTFETs) combine excellent electrical performance with robustness in harsh environmental conditions. The stochastic assembly of the one-dimensional nanomaterials with varying electronic properties allows intrinsic device-to-device variations that can be harnessed as a high-entropy source for PUFs [4, 5, 6]. Beyond individual characterization, CNTFETs can be integrated into larger, addressable structures suitable for scalable PUF implementations. In this work, we investigate such an integration, characterize the electrical behavior of the CNTFETs within the crossbar array, and explore the feasibility of interfacing its readout with an field-programmable gate array (FPGA) platform.

CPSWS'25: CPS Summer School PhD Workshop, September 22, 2025, Alghero, Sardinia, Italy
This work is partially supported by the German Research Foundation (DFG) within the priority program "Nano Security: From Nano-Electronics to Secure Systems" (SPP 2253) under project "NANOSEC^2: Nanomaterial-based platform electronics for PUF circuits with extended entropy sources" (439892735).

[*] Corresponding author.

martin.schmid@uni-passau.de (M. Schmid)

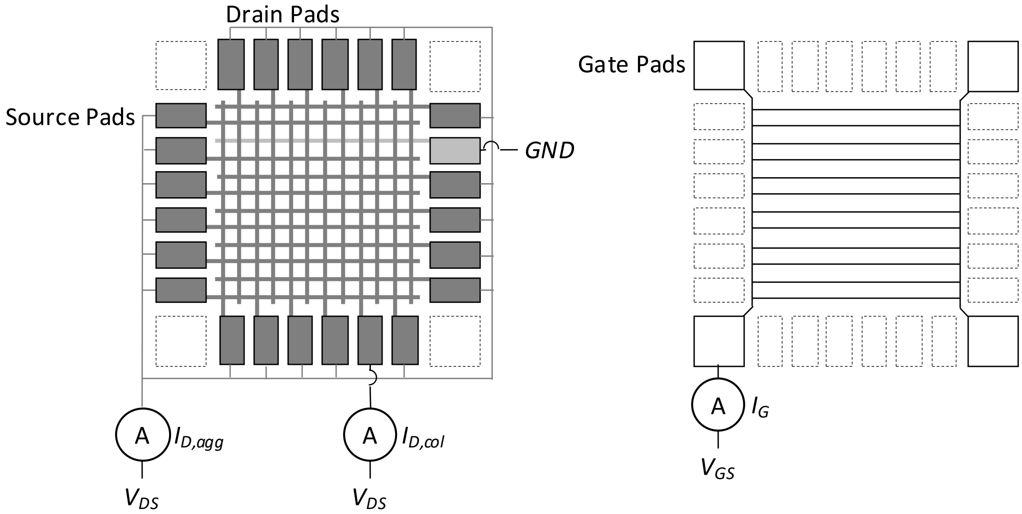

Figure 1: Layout of the 12 × 12 on-wafer CNTFET crossbar array. In the left panel, horizontal metal interconnects connect to the source terminals, and vertical interconnects connect the drain terminals of the CNTFETs at each intersection. The right panel shows the metal interconnects to the gate terminals, where the gates of all CNTFETs are electrically joined and routed to the four gate pads.

1.1. Problem statement

To ease the measurement process by reducing the number of required contact pads, we embedded the CNTFETs in an 12 × 12 on-wafer crossbar array, as illustrated in Figure 1. The CNTFETs are arranged into 12 rows, where the source terminals are connected horizontally and the drain terminals vertically. Further, the gate terminals of all CNTFETs are interconnected. The configuration shown on the left in Figure 1 illustrates the selective measurement of a single CNTFET: one source pad is connected to ground (GND), all other source and drain pads are biased to V_{DS}. Then, the current $I_{D,col}$ flowing into the drain pad connected to the drain of the selected transistor is measured using an ammeter (A). To derive a binary PUF response, a threshold is then chosen that uniformly groups the CNTFETs into a lower-current (*non-conducting*) and higher-current (*conducting*) set [4].

In an ideal scenario, the gate terminal of a CNTFET would be perfectly electrically isolated from its source and drain terminals. In practice, however, leakage currents can flow between the gate and the source or drain. In the crossbar configuration, such leakage affects the measurement of I_{DS} when currents are drawn from, or flow into, the measured drain column. As a result, the separation between conducting and non-conducting states in the individual CNTFETs becomes less distinct. While gate leakage also occurs in isolated CNTFETs, in that case, the effect is confined to the probed transistor and does not propagate through the array. In the interconnected crossbar, by contrast, the leakage influences multiple measurement paths, complicating the design of a universal quantization scheme based on a single threshold [4].

In this work, we evaluate leakage effects in the crossbar through comprehensive electrical measurements, outline how to derive an equivalent resistive circuit model to analyse parasitic currents, and present the future steps to improve the read-out architecture, including FPGA-based interfacing. The main contributions of this work are as follows:

- Electrical characterization of CNTFETs implemented in a 12×12 on-wafer crossbar array, including measurement of individual cell transfer characteristics and analysis of their behaviour within an interconnected structure.
- Suggestion of a method to identify and localize parasitic currents in the crossbar interconnect network, enabling differentiation between leakage paths and intrinsic cell behaviour.
- Proposal of an FPGA-based read-out architecture employing a voltage-readout active switch matrix, as outlined in the research plan, to facilitate scalable PUF evaluation and eventual integration into dedicated ICs.

1.2. Related Work

Hu *et al.* [5] fabricated a 2560 bit CNT-PUF which was constructed from fabricated 5x5 crossbar structures. They derived both a binary and ternary PUF with a mean intra-device Hamming distance of approximately 3%. Moon *et al.* [6] present a PUF constructed from all-printed carbon nanotube (CNT) networks. Rather than embedding individual CNTFETs into a crossbar, their design forms a network of dispersed CNTs enclosed by electrodes.

Practical system integration, such as into an FPGA-based platform, is still missing. We try to close this gap by analyzing a readout concept that can be interfaced with standard analog-to-digital converters (ADCs), enabling a more direct path toward integration into resource-constrained systems. While the progress to date was obtained from passive crossbar arrays using precision source-measure units (SMUs), the research plan outlines an active voltage-readout architecture currently in fabrication, designed to mitigate leakage effects, simplify measurement circuitry, and support scalable on-chip evaluation.

2. Methodology

To evaluate the electrical behaviour of the CNTFETs, we experimentally approximate their *transfer characteristics*, i.e., the relationship between their intrinsic drain current I_D and the gate-source voltage V_{GS} at a constant drain-source voltage V_{DS}. As the CNTFETs in the crossbar are not electrically isolated, I_D cannot be measured directly; instead, we approximate it by the current $I_{D,col}$ flowing into the corresponding drain column. For each of the 144 CNTFETs in the 12 × 12 crossbar array, we record the following quantities:

1. The electrical current $I_{D,col}$ measured at the drain pad connected to the drain terminal of the selected CNTFET including periphery when biased with V_{DS}.
2. The aggregate drain-source current $I_{D,\text{agg}}$ measured at all other source and drain pads when biased with V_{DS}.
3. The current I_G measured at the gate pads when biased with V_{GS}.

The transfer curve of the selected CNTFET derived from $I_{D,col}$ enables the assessment of its behaviour under various quantization models, by picking the required values from the curve. The additional two measurements provide insight into leakage currents propagated by the interconnected structure.

Measurements are performed directly on on-wafer crossbar structures using a wafer probing station equipped with a dedicated 28-needle probe card. All input/output lines are routed to a custom-built switch matrix [7], which selectively connects specific rows and columns of the crossbar to three precision SMUs. This configuration enables automated characterization of all CNTFETs in the array without repeated manual probe positioning, ensuring consistent measurement conditions across the dataset while maintaining practical measurement times.

3. Progress to Date

To date, we have characterized CNTFETs in more than 100 different crossbar arrays using $V_{DS} = \pm 0.5$ V over $V_{GS} \in \{2.0\text{ V}, 1.8\text{ V}, \dots, -2.0\text{ V}\}$, with a general current limit of 10 µA. The evaluated crossbars are categorized according to their fabrication parameters; in the following, we present results obtained from the arrays fabricated with the most promising parameter sets and that exhibit aforementioned leakage effects in their crossbar.

Figure 2 summarizes the results for the configuration $V_{DS} = -0.5$ V and $V_{GS} = \pm 2.0$ V. Each row in the left-side plots corresponds to the $I_{D,col}$ values measured for one crossbar, where each bar within a row represents the $I_{D.col}$ measurement for one CNTFET. The measured currents predominantly range from −200 nA to −0.1 nA. These results confirm the problem outlined in Section 1.1: while individually probed CNTFETs exhibited a clear separation between the two states in our previous work [4], this distinction in PUF response is much less pronounced in the crossbar configuration. This may be related

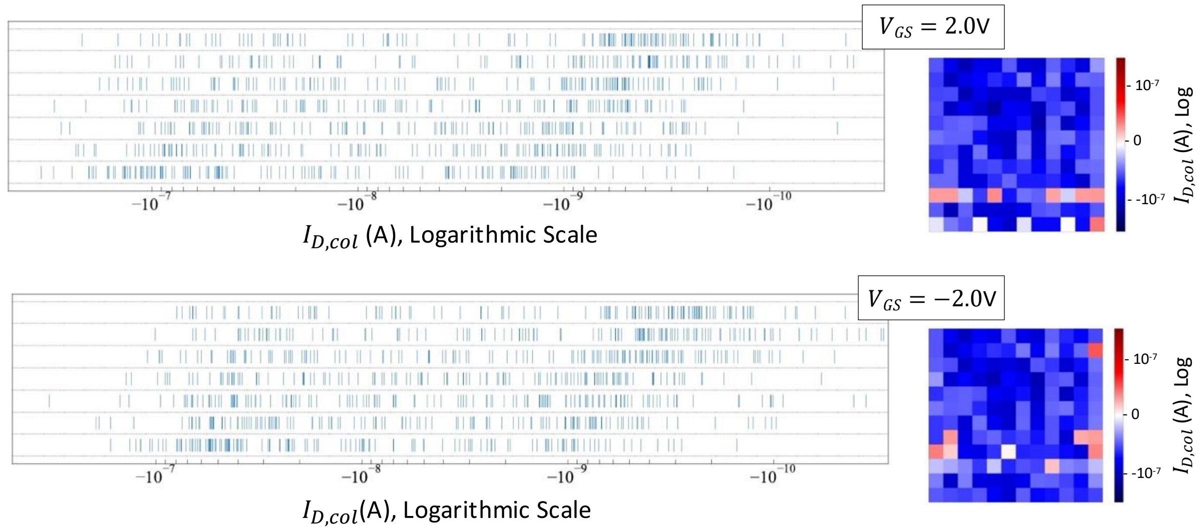

Figure 2: Measured $I_{D,col}$ currents for selected crossbars that exhibit leakage. In the left-hand scatter plots, each row corresponds to one crossbar, and each bar within a row represents the $I_{D,col}$ value measured for a selected CNTFET. A small number of currents lie outside of the displayed region (towards 0). The right-hand heatmaps visualize the same measurements as color maps, enabling analysis of spatial correlations within each crossbar. The upper plots show results for $V_{GS} = -2.0$ V, while the lower plots show results for $V_{GS} = 2.0$ V.

to the aforementioned leakage paths, which are assumed to scale with crossbar array size, complicating distinctive response for the used 12x12 crossbars.

Nonetheless, two distinct clusters can be observed for each structure, enabling the definition of a threshold for almost stable quantization. Table 1 lists the percentage of CNTFETs classified as conducting under various $I_{D,col}$ thresholds, derived from the transfer characteristics shown in Figure 2. Among the presented crossbars, the most stable quantization occurs at a threshold of approximately −6 nA to −5 nA, where the change in the proportion between conducting versus non-conducting is minimal. Crossbars A-C exhibit a strong bias toward non-conducting CNTFETs, while crossbar H is biased toward conducting transistors. The remaining crossbars achieve an acceptable uniformity of around 45% conducting cells. Still, error-correcting measures such as cell selection would be required to achieve perfect uniformity, thereby reducing the available PUF response width.

Table 1

Percentage of cells with $I_{D,col}$ currents below the specified thresholds for select measured crossbar array at $V_{DS} = -0.5$V and $V_{GS} = 2.0$V. For each row, bold percentages indicate the point with the smallest difference to the neighboring percentages.

Crossbar	$\mathbf{I_{D,col}} < -8$ **nA**	< -7 **nA**	< -6 **nA**	< -5 **nA**	< -4 **nA**
A	22%	24%	26%	**27%**	27%
B	24%	24%	26%	**27%**	27%
C	33%	34%	**35%**	36%	38%
D	35%	39%	42%	**43%**	45%
E	41%	42%	**44%**	**45%**	47%
G	46%	48%	**48%**	49%	51%
H	61%	61%	64%	**65%**	65%

4. Plan of research

4.1. Leakage localization via equivalent circuit modelling

In order to analyse the leakage behaviour observed during measurements, the recorded current values are used to mathematically derive an equivalent resistive circuit of the crossbar array for a given (V_{DS}, V_{GS}) configuration. The resistances are approximated iteratively such that the simulated network reproduces the experimentally measured currents. The equivalent circuit model provides a spatial map of the array, highlighting cells that exhibit excessive gate leakage or short circuits between their terminals. This could be an perspective standard proccess during enrollment of the PUF in order to support cell selection for initial trimming and entropy improvement.

As an illustrative example, Figure 3 shows a proof-of-concept simulation performed on a 2×2 subsection of the array. In this preliminary model, resistance values were adjusted manually to qualitatively reflect leakage phenomena observed during measurements. It demonstrates how the equivalent circuit approach can reveal abnormal leakage paths and localize them to specific cells and terminals. In the minimal-leakage case (left), current flows through the measured CNTFET as well as through the other CNTFETs in the grounded source row. In the leakage case (right), additional current from the gate flows into the drain column, reversing the sign of $I_{D,col}$. Depending on the location of the gate leakage relative to the measured CNTFET and the corresponding recorded values, these leakage paths can reliably be identified.

4.2. Characterization of voltage-readout active switch matrix

To enable crosstalk-free addressing of individual PUF cells, the passive crossbar structure will be extended to an active matrix. In this design, the PUF circuitry is placed inside a cell activated by thin-film FETs, allowing selective activation of individual CNTFETs. Further, it includes an adjustable potentiometer that enables read out of voltages instead of currents. The goal is to distinguish an additional state from the fully conducting and fully insulating states. This enables ternary response extraction, which can increase the entropy per cell and provide a richer feature set for PUF evaluation. The layout for this structure has already been finalized, and the corresponding wafers are currently in fabrication.

4.3. FPGA interfacing

Building upon the voltage-readout active switch matrix described in the previous section, the analog output voltages of the selected CNTFET cells will be digitized using an FPGA with integrated multichannel ADCs. Within the FPGA, the digitized outputs will be processed to perform binary or ternary

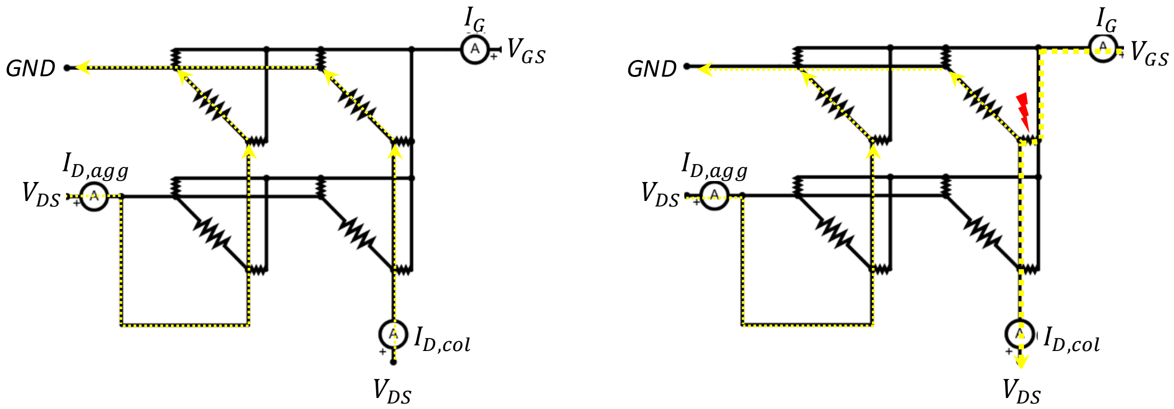

Figure 3: Illustrative 2×2 proof-of-concept simulation for leakage localization. The left panel represents a structure with minimal gate leakage, while the right panel shows a case in which the gate of one CNTFET leaks into the measured drain column. Yellow dotted arrows indicate the dominant current paths.

quantization. For binary quantization, a single threshold voltage will be applied to the digitized value. For ternary quantization, the same CNTFET will be measured twice—once in the gate-on state and once in the gate-off state and the resulting digitized valus compared. The FPGA-based approach serves as an intermediate prototyping step toward eventual integration of the PUF into a dedicated IC.

4.4. Security evaluation

In the final stage, the integrated PUF system will be subjected to a comprehensive security evaluation. First, potential vulnerabilities to power analysis will be investigated. In particular, the effect of electromagnetic (EM) emanations [8] from the read-out lines will be examined. In addition, we plan to evaluate the susceptibility of the system to intentional EM injection attacks [9]. These effects will be compared for serial versus parallel read-out, as the latter might blend the individual states enough to make an effective attack impossible.

Beyond electrical side-channel analysis, optical probing via photon emission microscopy [10] will be applied to the crossbar to detect localized switching activity that may reveal individual cell states. Environmental stability will be assessed by measuring the PUF under controlled variations in temperature and humidity to determine their impact on the analog outputs, quantized responses, and reliability metrics.

4.5. Critical Issues and Mitigation

Fabrication delays, electrotechnical faults or lack of precise equipment may conflict with the desired goals of the research. The voltage-readout active switch matrix may exhibit electrotechnical limitations, such as leakage through the thin-film transistors. Further, the differential between the output voltage of conductive and non-conducting cells may be too minor to accurately be distinguished by the ADCs in customer-grade FPGAs. Should this occur, an FPGA interface can still be designed and validated under the assumption of a theoretical PUF that produces idealized output values. Similarly, the security evaluation can be carried out on the readout circuitry in isolation, without requiring a fully functional PUF.

5. Conclusion

This work addresses the challenge of reliably extracting PUF responses from CNTFETs integrated in an 12x12 interconnected crossbar array. While individually probed CNTFETs exhibit a clear distinction between conducting and non-conducting states, measurements in the crossbar configuration revealed reduced separation due to parasitic currents propagating through the shared wirings. In particular, gate leakage in a single CNTFET can influence multiple measurement paths, altering the transfer characteristics of neighbouring cells and degrading the quality of the derived PUF responses. In response, we derived a new measurement procedure that additionally records the aggregate currents flowing to the non-selected drain and source pads of the crossbar array. This aids in identifying the points of leakage inside the structures.

The next intermediate milestone in this project is the implementation of a leakage-localization method based on equivalent resistive circuit modelling, in parallel to the preparation of a measurement setup for the voltage-readout active switch matrix currently in fabrication. These steps will provide the foundation for evaluating improved read-out architectures and their integration with FPGA-based processing in cyber-physical systems.

Declaration on Generative AI

During the preparation of this work, the authors used Grammarly and Chat-GPT4 and Chat-GPT5 for sentence polishing. After using these tools, the authors reviewed and edited the content as needed and take full responsibility for the publication’s content.

References

[1] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. Van Dijk, S. Devadas, A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications, in: 2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No. 04CH37525), IEEE, 2004, pp. 176–179.

[2] B. Skoric, G.-J. Schrijen, P. Tuyls, T. Ignatenko, F. Willems, Secure Key Storage with PUFs, in: Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting, Springer, 2008, pp. 269–292.

[3] J. Kong, F. Koushanfar, P. K. Pendyala, A.-R. Sadeghi, C. Wachsmann, PUFatt: Embedded Platform Attestation Based on Novel Processor-Based PUFs, in: Proceedings of the 51st Annual Design Automation Conference (DAC), 2014, pp. 1–6.

[4] S. Böttger, F. Frank, N. A. Anagnostopoulos, A. Mohamed, M. Hartmann, T. Arul, S. Hermann, S. Katzenbeisser, CNT-PUFs: Highly Robust Physical Unclonable Functions Based on Carbon Nanotubes, in: 2023 IEEE 23rd International Conference on Nanotechnology (NANO), IEEE, 2023, pp. 1–6.

[5] Z. Hu, J. M. M. L. Comeras, H. Park, J. Tang, A. Afzali, G. S. Tulevski, J. B. Hannon, M. Liehr, S.-J. Han, Physically Unclonable Cryptographic Primitives Using Self-Assembled Carbon Nanotubes, Nature Nanotechnology 11 (2016) 559–565.

[6] D.-I. Moon, A. Rukhin, R. P. Gandhiraman, B. Kim, S. Kim, M.-L. Seol, K. J. Yoon, D. Lee, J. Koehne, J.-W. Han, et al., Physically Unclonable Function by an All-Printed Carbon Nanotube Network, ACS Applied Electronic Materials 1 (2019) 1162–1168.

[7] F. Frank, N. A. Anagnostopoulos, S. Böttger, S. Hermann, T. Arul, S. G. Stavrinides, S. Katzenbeisser, A Dedicated Mixed-Signal Characterisation and Testing Framework for Novel Digital Security Circuits That Use Carbon-Nanotube-Based Physical Unclonable Functions, in: 2022 11th International Conference on Modern Circuits and Systems Technologies (MOCAST), IEEE, 2022, pp. 1–4.

[8] D. Agrawal, B. Archambeault, J. R. Rao, P. Rohatgi, The EM Side—Channel(s), in: International Workshop on Cryptographic Hardware and Embedded Systems (CHES), Springer, 2002, pp. 29–45.

[9] F. Wan, F. Duval, X. Savatier, A. Louis, B. Mazari, Effects of Conducted Electromagnetic Interference on Analogue-to-Digital Converter, Electronics Letters 47 (2011) 23–25.

[10] D. Nedospasov, J.-P. Seifert, C. Helfmeier, C. Boit, Invasive PUF Analysis, in: 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), IEEE, 2013, pp. 30–38.