Carbon-Nanotube-Based Physical Unclonable Functions and True Random Number Generators

Nikolaos Athanasios Anagnostopoulos*, Tolga Arul*†, Simon Böttger‡, Florian Frank*,
Ali Mohamed‡, Martin Hartmann‡, Sascha Hermann‡§, Stefan Katzenbeisser*
*University of Passau, Faculty of Computer Science and Mathematics, Innstraße 43, 94032 Passau, Germany
Emails: {Nikolaos.Anagnostopoulos, Tolga.Arul, Florian.Frank, Stefan.Katzenbeisser}@uni-passau.de
†Technical University of Darmstadt, Computer Science Department, Hochschulstraße 10, 64289 Darmstadt, Germany
Email: arul@rbg.informatik.tu-darmstadt.de
‡Chemnitz University of Technology, Center for Microtechnologies, Reichenhainer Str. 70, 09126 Chemnitz, Germany
Emails: {simon.boettger, ali.mohamed, martin.hartmann, sascha.hermann}@zfm.tu-chemnitz.de
§Fraunhofer Institute for Electronic Nano Systems (ENAS), Technologie-Campus 3, 09126 Chemnitz, Germany
Email: sascha.hermann@enas.fraunhofer.de

***Abstract*—In this work, we present a novel way of increasing the entropy of the CNT-PUF, a Physical Unclonable Function (PUF) based on a monolithic array of 144 Carbon-NanoTube Field Effect Transistors (CNT-FETs), arranged in a 12×12 crossbar structure. We note that the responses of this PUF are based on the electrical characteristics of the relevant CNT-FETs. More specifically, the drain current I_D of each CNT-FET under the influence of a particular gate-source voltage V_{GS} indicates, through the use of a threshold value, whether each relevant CNT cell of the array is conducting (acting either as a true conductor or as a semiconductor) or not (acting as an insulator). In this work, we propose the adoption of individual threshold values for each such cell as part of the relevant PUF challenge, thereby significantly increasing the entropy of this PUF.**

***Index Terms*—Carbon NanoTube (CNT), Physical Unclonable Function (PUF), True Random Number Generator (TRNG), hardware security, security, Internet of Things (IoT), increased entropy, increased stability**

I. Introduction and Related Work

With the advancement of the Internet of Things (IoT), which allows devices to directly exchange information and take actions based on this information without the direct intervention of people, the demand for security has significantly increased. In particular, as the IoT brings together both high-end devices, e.g., infrastructure servers, and really resource-constrained ones, such as single-board computers and microprocessors, used solely for the collection of sensor data, the need for lightweight security has grown remarkably.

To this end, Physical Unclonable Functions (PUFs) [1] have been proposed as a hardware-based security solution that can allow for the realisation of low-cost security anchors that can provide highly unique and unpredictable cryptographic tokens, such as encryption keys. Moreover, such nanomaterials as Carbon NanoTubes (CNTs) have already been utilised for the creation of PUFs [1], [2], as such PUFs can be more robust and tamper-resistant in comparison to ones based on silicon, while at the same time being compatible with the complementary metal-oxide-semiconductor (CMOS) fabrication process of electronic devices.

Hence, in a recently submitted work [3], we have proposed the CNT-PUF, a PUF based on the characterisation, through a threshold I_D value, of the cells of a monolithic 12×12 array of CNT-FETs as either conductive (acting either as true conductors or as semiconductors) or non-conductive (acting as insulators). The cells belonging to the former category are assigned the logical value of 1 and the ones belonging to the latter, the logical value of 0, leading to a 144-bit PUF response that has proven to be extremely stable.

In this work, we propose a novel classification method for the CNT-PUF based on the adoption of an individual threshold value for each CNT-PUF cell, which forms part of the relevant PUF challenge. In this way, our work makes the following contributions:

1) It offers higher flexibility for creating cryptographic tokens, such as keys, by significantly increasing the overall entropy of the CNT-PUF Challenge-Response Pairs (CRPs).
2) It also allows for even higher stability of the overall response of the CNT-PUF, as long as each individual threshold is chosen to be far away from the region in which the I_D values recorded for the relevant cell occur.
3) Moreover, it provides for the potential restoration of the security of the CNT-PUF, even when the attacker has gained knowledge on particular sets of its CRPs.
4) Finally, it can be used to convert the CNT-PUF into a source of higher entropy that can serve as a True Random Number Generator (TRNG).

The remainder of this work is structured as follows. Section II provides an overview of the fundamentals of the operation

This work has been partially funded by the German Research Foundation – Deutsche ForschungsGemeinschaft (DFG), as part of the Projects "PUFMem: Intrinsic Physical Unclonable Functions from Emerging Non-Volatile Memories" (project number 440182124) and "NANOSEC: Tamper-Evident PUFs based on Nanostructures for Secure and Robust Hardware Security Primitives" (project number 439892735) of the Priority Program "Nano Security: From Nano-Electronics to Secure Systems" (SPP 2253), and by the Interreg VI-A Programme Germany/Bavaria–Austria 2021–2027 – Programm INTERREG VI-A Bayern–Österreich 2021–2027, as part of the Project "CySeReS-KMU: Cyber Security and Resilience in Supply Chains with focus on SMEs" (project number BA0100016).

[1]The term "Physical Unique Function" can more accurately describe a PUF.

of the CNT-PUF. Section III discusses the novel classification method as well as the advantages associated with it. Finally, in Section IV, we summarize our contributions and provide an outlook for future work, thereby concluding this work.

II. Background Information

The operation of a PUF is based on the existence of CRPs that are unique per device and rather unpredictable. In particular, a PUF can be described as a physical object with unique and rather unpredictable characteristics, which are most often induced in the physical object by minor variations during its manufacturing process. Under particular conditions and actions, e.g., by providing some input if the PUF is an electronic circuit, to which we refer as the PUF challenge, a PUF provides the current values of its defining characteristics – in the case of the PUF being an electronic circuit, potentially as logical values at its output; we refer to those values as the PUF response, and in the case of PUFs consisting of electronic circuits, they are binary.

In the case of the CNT-PUF, as already mentioned, the PUF response is based on the electrical characteristics of the relevant CNT-FETs, each of which constitutes a cell of the overall 12×12 monolithic crossbar array. In particular, the drain current I_D of each CNT-FET is measured under the influence of a gate-source voltage V_{GS} equal to $-2.5V$. Nevertheless, it has been observed that the measurements of I_D inherently incorporate some noise, leading to slightly different values for the same cell, even for the exact same value of V_{GS}. However, as such measurement values tend to concentrate within a limited region, each cell is assigned a logical value based on whether the measured I_D value is above or below a threshold value that is common for all cell measurements, as shown in Figure 1, where the dashed grey lines indicate the range in which the authors of [3] propose that the common I_D threshold value is set [2]. The concatenation of the logical values assigned to all the cells form the response of this PUF, with the provided V_{GS} and the order in which the CNT-FET cells are measured, as well as other relevant conditions, such as the ambient temperature, forming the relevant PUF challenge.

As it is evident, this method allows only for the production of a single 144-bit binary response for each crossbar array.

III. Carbon-Nanotube-Based Security Primitives of Increased Entropy

As shown in Figure 2, applying a common I_D threshold value (shown as a red line, within the range in which the authors of [3] propose that the common I_D threshold value is set, which is indicated by the grey dashed lines), can lead to responses containing erroneous bits. On the contrary, by utilising different I_D threshold values for each CNT-FET cell, as shown in Figure 3 through nine randomly selected cells, errors can be avoided with extremely high probability. Additionally, a fully unstable response can also be produced to generate a TRNG, e.g., by using the green threshold set of Figure 3 that separates the measurement sets of all the CNT-FET cells in the middle. Utilising this method, it is possible to generate either a TRNG, or a stable or unstable PUF response. Additionally, it is even possible to determine the potential bias towards either of the logical values for both a TRNG and a PUF response produced using this method. Moreover, it is even possible to determine the degree of instability of the PUF response and, in any case, a fully stable response can be generated using this method.

We also note that, as Figure 3 shows through nine randomly selected cells, different threshold sets leading to fully stable responses can be utilised (such as the purple, pink, and brown threshold sets shown in Figure 3, leading to stable, but different responses. In particular, the purple set produces a '111011011' response, the pink one a '001100011' response, and the brown one a '010010010' response, leading to fractional Hamming distances between $\frac{4}{9}$ and $\frac{5}{9}$, i.e., to perfectly unique/distinct responses [3]. In this way, it is proven that this classification method significantly increases the overall entropy of the CNT-PUF.

Finally, as the purple, pink, and brown threshold sets shown in Figure 3 lead to perfectly unique/distinct responses, they can also be utilised to restore the security of the CNT-PUF, as even if a response produced by one of these threshold sets becomes known to the attacker, the other two can still be utilised without any security compromise.

IV. Conclusion and Future Work

In this work, we have presented a novel way of classifying the I_D measurements used to form the response of the CNT-PUF that has been described in [3]. This method significantly increases the overall entropy of this PUF, offering the ability to generate an increased number of cryptographic tokens. It also allows for even higher stability of the responses produced by this PUF. Moreover, it can also be used to restore the security of the PUF, when an attacker knows some of the CNT-PUF's CRPs. Finally, it can also be used to transform the CNT-PUF structure into a TRNG. Thus, we believe that the described method really enhances the operation of the CNT-PUF. Future work should measure the entropy and stability increase that occurs when our classification method is used, and assess the potential cost required for storing the information concerning the limits of the region that the I_D values recorded for each CNT-FET cell occupy.

References

[1] Z. Hu, J. M. M. L. Comeras, H. Park, J. Tang, A. Afzali, G. S. Tulevski, J. B. Hannon, M. Liehr, and S.-J. Han, "Physically unclonable cryptographic primitives using self-assembled carbon nanotubes," *Nature nanotechnology*, vol. 11, no. 6, pp. 559–565, 2016.

[2] Essentially, cells providing a high I_D, whose CNTs act as true conductors or semiconductors, are assigned the logical value of 1, and cells providing a low I_D, whose CNTs act as insulators, are assigned the logical value of 0.

[3] Thus, such responses could also be directly used as cryptographic tokens, such as keys.

[2] E. Burzurí, D. Granados, and E. M. Pérez, "Physically Unclonable Functions Based on Single-Walled Carbon Nanotubes: A Scalable and Inexpensive Method toward Unique Identifiers," *ACS Applied Nano Materials*, vol. 2, no. 4, pp. 1796–1801, Apr 2019. [Online]. Available: https://doi.org/10.1021/acsanm.9b00322

[3] S. Böttger, F. Frank, N. A. Anagnostopoulos, T. Arul, A. Mohamed, M. Hartmann, S. Hermann, and S. Katzenbeisser, "CNT-PUFs: Highly robust and heat-tolerant carbon nanotube-based physical unclonable functions," submitted for publication.

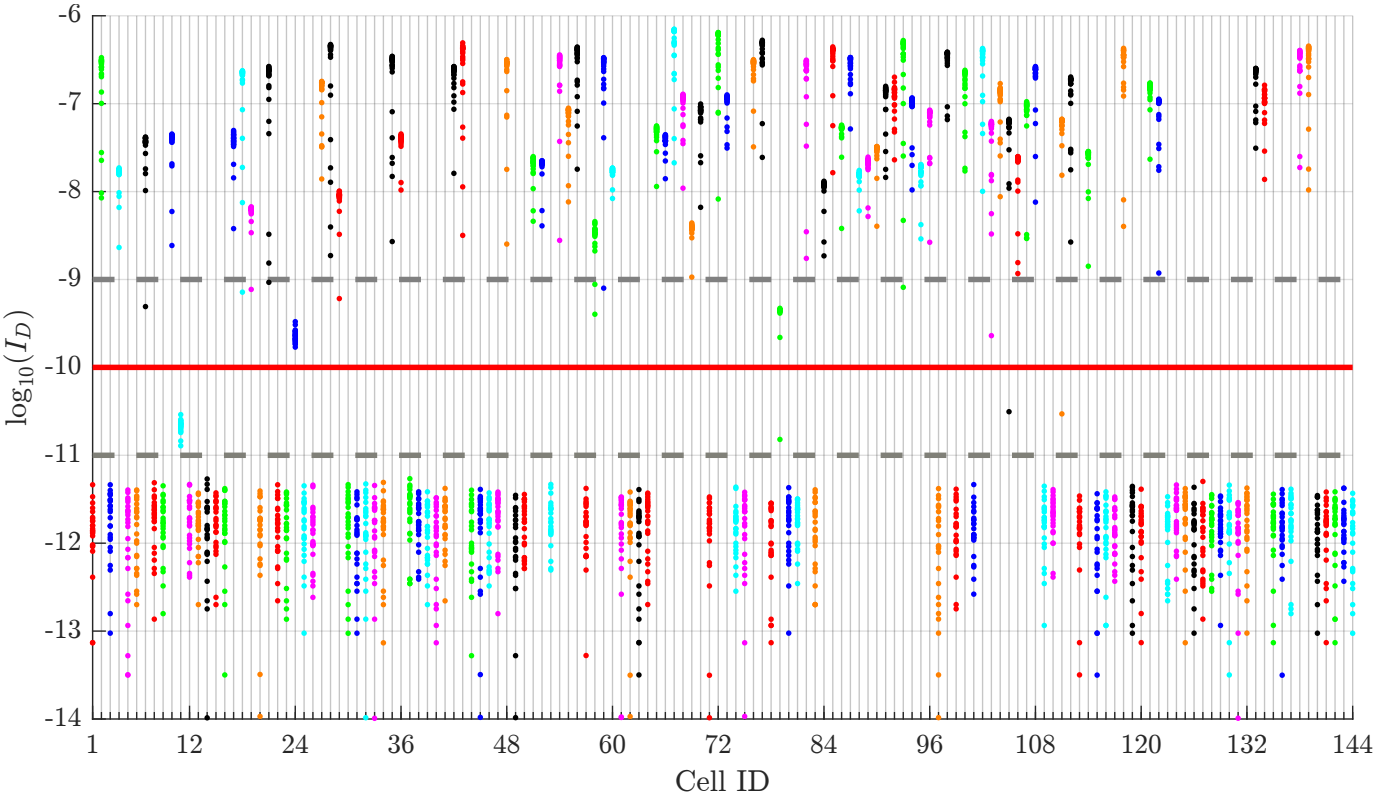

Fig. 1. Distribution of 28 measurements of the drain current I_D for each CNT-FET when applying a V_{GS} = -2.5V and V_D = -1V. One can retrieve the stability of each PUF cell from this figure, as well as the overall distribution of conducting and non-conducting CNT-FETs of the examined device, for V_{GS} = -2.5V and V_D = -1V, based on a threshold value for I_D. In [3], it is suggested that a common threshold be applied in the range indicated by the dashed grey lines. Such an exemplary threshold could be the one indicated by the red solid line.

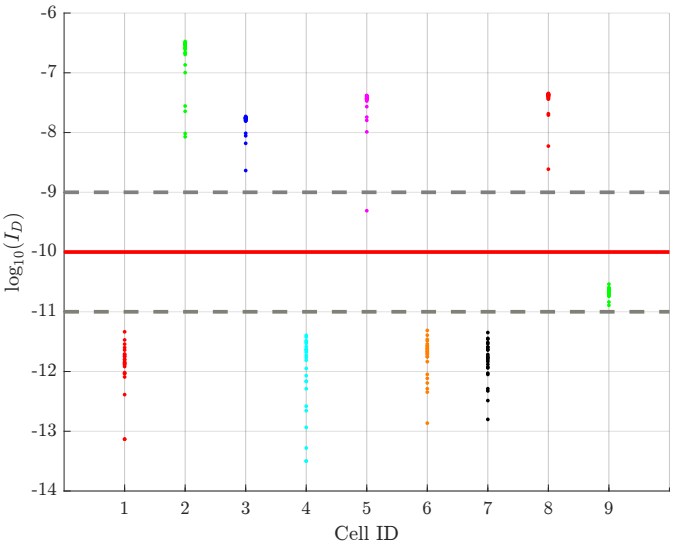

Fig. 2. Distribution of the 28 measurements of the drain current I_D for a random selection of nine CNT-FET cells, from Figure 1, when applying a V_{GS} = -2.5V and V_D = -1V. A threshold shown as a red line has been selected within the range defined by the dashed grey lines, leading to a PUF response of '011010010'. Note that if the red line threshold separated the measurements of the selected ninth cell, the response produced could have one erroneous bit.

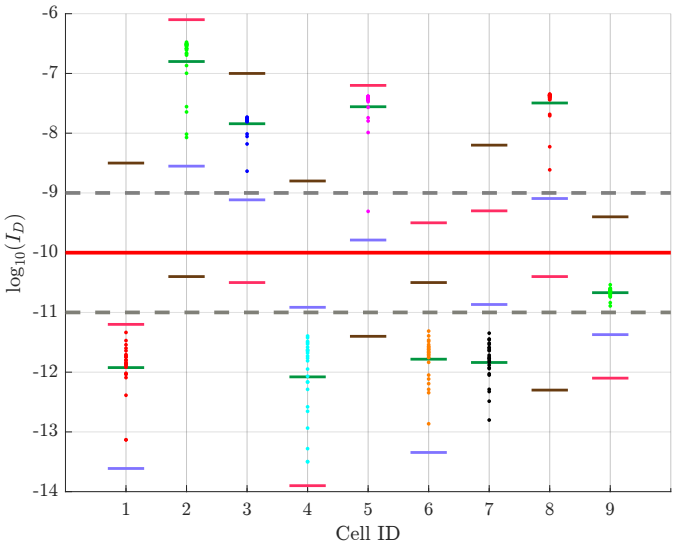

Fig. 3. Distribution of the 28 measurements of the drain current I_D for the nine CNT-FET cells shown in Figure 2 when applying V_{GS} = -2.5V and V_D = -1V. Individual thresholds are applied to each cell, shown as purple, green, pink and brown line segments, forming four sets of thresholds. The green set leads to a TRNG behaviour, as it separates all sets of measurements. The other three sets lead to PUF responses that demonstrate a fractional Hamming distance from 0.4 to 0.6 when compared.