A Dedicated Mixed-Signal Characterisation and Testing Framework for Novel Digital Security Circuits That Use Carbon-Nanotube-Based Physical Unclonable Functions

Florian Frank*, Nikolaos Athanasios Anagnostopoulos*†, Simon Böttger‡,
Sascha Hermann‡§, Tolga Arul*†, Stavros G. Stavrinides¶, Stefan Katzenbeisser*

*University of Passau, Faculty of Computer Science and Mathematics, Innstraße 43, 94032 Passau, Germany
Emails: {Florian.Frank, Nikolaos.Anagnostopoulos, Tolga.Arul, Stefan.Katzenbeisser}@uni-passau.de
†Technical University of Darmstadt, Computer Science Department, Hochschulstraße 10, 64289 Darmstadt, Germany
Emails: {na45tisu, arul}@rbg.informatik.tu-darmstadt.de
‡Chemnitz University of Technology, Center for Microtechnologies, Reichenhainer Str. 70, 09126 Chemnitz, Germany
Emails: {simon.boettger, 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
¶School of Science and Technology, International Hellenic University, Thermi Campus, 57001 Thessaloniki, Greece
Email: s.stavrinides@ihu.edu.gr

***Abstract*—Our work proposes a characterisation and testing methodology, as well as the relevant custom implementation, for measuring novel digital security circuits that use nanomaterial-based Physical Unclonable Functions (PUFs) as their security anchors. Although in this work we focus on PUFs that utilise the electrical characteristics of a crossbar structure of Carbon NanoTube (CNT) cells, the proposed methodology is applicable to most, if not all, PUFs that are based on similar crossbar structures of nanomaterials. Our work describes and discusses in detail the relevant characterisation and testing framework, while also presenting the corresponding mixed-signal circuit implementation, which can be utilised to provide a digital security token in an automated manner. Finally, preliminary results concerning the considered CNT PUFs are also presented, proving in this way the ability of the proposed framework to be utilised for the characterisation and testing of these PUFs, as well as for the implementation of security applications in the context of embedded systems and the Internet of Things (IoT), using nanomaterial-based PUFs in general.**

***Index Terms*—Digital circuit, security, Physical Unclonable Function (PUF), Carbon NanoTube (CNT), mixed-signal circuit, testing, characterisation, measurement automation, nanomaterial**

I. Introduction

In recent years, the advancing digitalisation of systems and services has paved the way for the widespread adoption of the Internet of Things (IoT), i.e., of a network where information is exchanged between devices without human intervention. In the context of the IoT, information gathered from sensor devices is transmitted to other devices for computation, which in turn, leads to commands being issued to actuator devices. The pervasive nature of the IoT has brought forward the consolidation and synergy of different systems and services that allow for advanced applications.

In this framework, the security of IoT devices and embedded systems, especially the ones utilised in edge computing, is emerging as a critical issue for the expansion of the IoT ecosystem. Moreover, the need for cost-efficient security in the context of embedded and cyber-physical systems, the IoT, as well as the Industry 4.0/5.0 applications, services, and systems, becomes highly evident, as, otherwise, it may be possible for a malicious adversary to modify, damage, and/or cause such systems to malfunction, and the relevant applications and services to fail.

At the same time, the use of advanced nanomaterials in commercial and industrial electronics has increasingly grown [1], due to the favorable properties of nanomaterials, and their ability to function as an improved form of current electronic components, e.g., transistors, or as novel electronic components, e.g., memristors. However, due to their high intrinsic variability, nanomaterial-based devices allow for the implementation of advanced hardware-embedded security anchors, such as Physical Unclonable Functions (PUFs), that can be used to provide security applications, even for resource-constrained devices, in a practical and cost-efficient manner.

PUFs utilise the characteristics of physical objects, such as nanomaterial-based devices, in order to obtain a behaviour that is highly unique per device instance, and thus identifiable.

This work has been 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).

In particular, such nanomaterial-based devices as Carbon-NanoTube-based Field-Effect Transistors (CNT-FETs) have an enormous potential for shaping a new class of miniaturized, low-power, and multi-bit security components, such as PUFs, of the highest entropy and robustness [2], which may also provide tamper-evidence capabilities.

To this end, a dedicated methodology that will allow for the characterisation and testing of such devices as security mechanisms in a quick and efficient manner, needs to be developed. Hence, in this work, we propose such a dedicated framework for the realisation and testing of such novel PUFs, which utilizes a mixed-signal approach, i.e., an analog measurement and testing setup that is controlled by a digital development platform and further coordinated by a computer. The measurement procedure has been implemented on advanced nanomaterial devices, i.e., CNT-FETs; devices that although operate in the digital domain (transistor mode), they provide an analog fingerprint response, which, however, can be easily transformed into a digital security token.

II. Layout of the Carbon-Nanotube PUF

The examined PUF is based upon the electrical characteristics of a crossbar array of CNT-FET cells. For the purposes of our research, a relatively large number of CNT-FET crossbar arrays, each of which consists of 12 rows and 12 columns as shown in Figure 1, have been implemented on pre-structured 200mm silicon wafers. Groups of these 144-bit CNT-based PUFs are manufactured with different configurations, like different channel widths or speeds in inserting the carbon nanotubes in a reproducible process. This process causes some minor differences that change the electrical characteristics of each CNT-FET, so that a highly unique response is produced. Also the influence of the different configurations on the electric characteristics is analyzed, to optimize the process to achieve the highest possible entropy in these PUF responses.

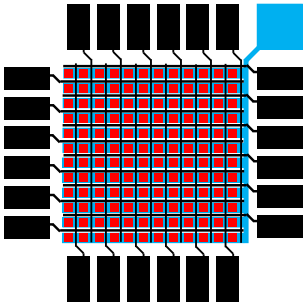

Fig. 1. Schematic view of the crossbar array of carbon nanotube cells that is used as a PUF. Each red square represents a CNT-FET cell, while the black rectangles and lines represent the metal pads and wires, respectively, that are used to enable access to the cells. The blue square and lines represent the global gate V_{GS} pad and the relevant wires, respectively. All the wires are isolated in such a way as to allow access to each individual cell without significantly affecting nearby wires and cells.

III. The Characterisation and Testing Framework

Toward the quick and efficient characterisation and testing of such chips (nanomaterial crossbar arrays), we propose a methodology based upon the selection of individual cells using a switch matrix, and the swift measurement of the electric characteristics of each cell. In particular, in the case of CNT-FET cells, the drain current of each cell is measured while different gate and drain voltages are applied. To this end, we have designed and implemented a novel measurement setup consisting of two principal components: a motherboard and a daughterboard, which are connected to each other through a Peripheral Component Interconnect Express (PCI-E) interface. In this way, the motherboard can be utilised to select particular cells on the relevant PUF chip that each daughterboard provides an interface to. The motherboard itself provides an interface between each of the removable daughterboards and the measurement equipment, hence allowing for the readout and characterisation of individual PUF cells.

A. The Daughterboard: An Autonomous Interface for Each PUF Instance

In our framework implementation, each 12×12 CNT crossbar array is placed on the central pad of a daughterboard (shown in Fig. 2), and connections to the surrounding pads are established by ultrasonic wedge bonding. The connections of these pads are forwarded to a PCI-E M.2 M-Key interface. Here, all PCB wires, except for the ones connected to the ground and the global gate pin, are routed in such a way that they have the same length, and the use of vias is avoided. This allows us to make precise and comparable measurements that are not distorted by any variations in the PCB wire resistance.

Each daughterboard has a size of 41mm×41mm, and all its wire tracks, except for the ground and gate wires, have a length of 100mm. Finally, it should be mentioned that these boards were produced with an Electroless Nickel / Immersion Gold (ENIG) surface finish, so that the PCB would have a planar surface suitable for wire bonding.

Fig. 2. The daughterboard, which acts as an interface between the motherboard and the CNT-FET crossbar array. The daughterboard is connected to the motherboard through a PCI-E socket.

B. The Motherboard: An Interface Between the Measurement Devices and the Daughterboard

The motherboard, which is shown in Fig. 3, is responsible for selecting a CNT PUF cell by its row and column position, and further forwarding the row and column connections to the dedicated measurement device that plays the role of the Source Measure Unit (SMU), a Keithley 2636B SMU.

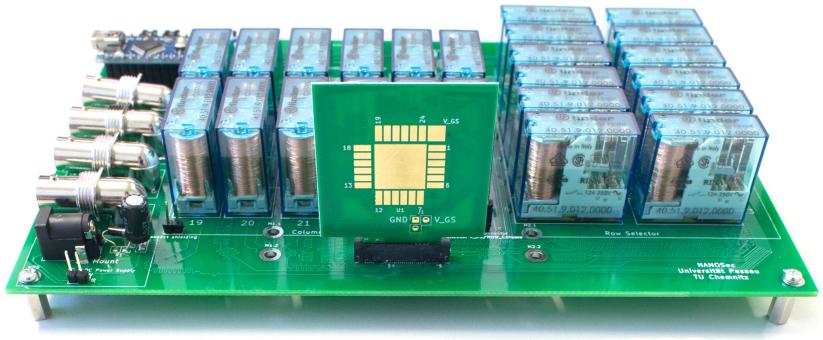

Fig. 3. The motherboard, which is used in order to select individual CNT-FETs on the relevant crossbar array that is attached and connected to the daughterboard. Measurements are performed by a Source Measure Unit (SMU) connected to the motherboard.

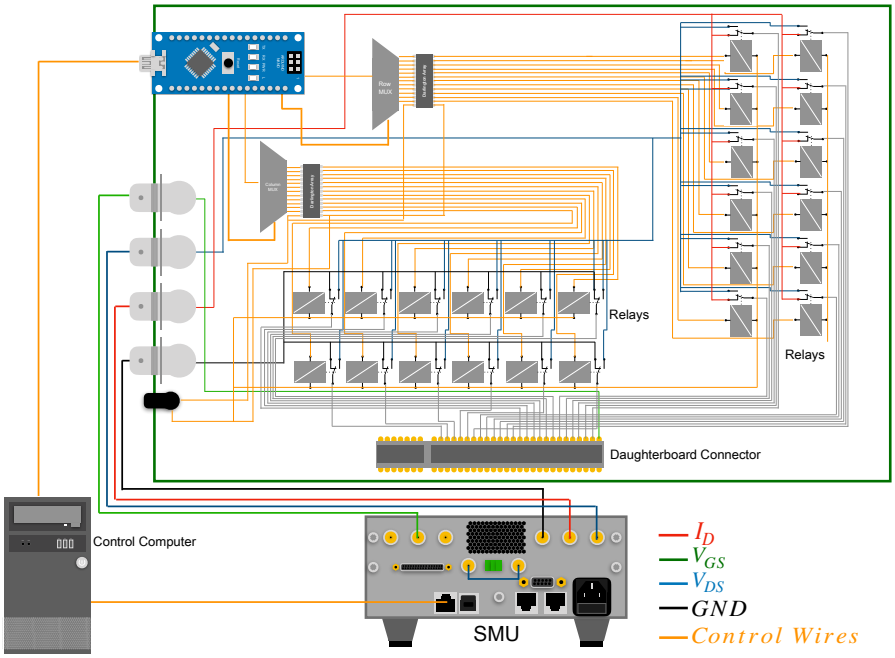

Fig. 4. An overview of the framework implementation of the proposed characterisation and testing methodology.

The motherboard provides a PCI-E M.2 M-Key socket, so that multiple daughterboards can be easily exchanged. This allows the swift measurement of the CNT-FET crossbar arrays independently and in a sequential manner.

The selection of a specific CNT-FET is performed by an Arduino Nano, using a particular relay for the row selection and another for the column selection, so that a direct connection is established between the SMU and the selected cell. The relays used in this case are Single Pole Double Throw (SPDT), due to their ability to establish a connection without a large amount of parasitic resistance as they can be completely switched on and off, in contrast to solid state switching devices, e.g., transistors. To measure a cell, the SPDT relays are used to apply I_D to the selected column and to connect the selected row with GND, as well as to apply V_{DS} to all the other rows and columns (which are not selected), in order to prevent parasitic resistances from affecting the measurement.

C. The Overall Measurement Circuit Design

The overall measurement system is presented in Fig. 4. The system includes a computer controlling both the SMU (the dedicated measurement device) and the circuit controlling the measurement, i.e., the motherboard. In order to measure a cell, the external computer selects a row and a column on the crossbar structure by communicating with the Arduino Nano (contained in the motherboard), which is responsible for switching the relays so that the appropriate connections are made. The Arduino board forwards the selection command through GPIO pins to a pair of Analog Devices ADG726 multiplexers, each of which has 16 channels. These multiplexers select the relevant cell, which is driven by a Darlington array connected to 12 V DC via a barrel jack connector (shown as a black cylinder on Fig. 4). Then, the computer system captures the relevant measurement data through a connection to the Keithley 2636B SMU. The orange lines in Fig. 4 signify the corresponding control wires, which are used either to control the switching of the relays or to control the Arduino Nano and the SMU. This way, an automated mixed-signal characterisation and testing setup is implemented with a fully configurable logic, which allows for the direct measurement of each of the carbon nanotube cells within each CNT-FET array that has been bound to a daughterboard.

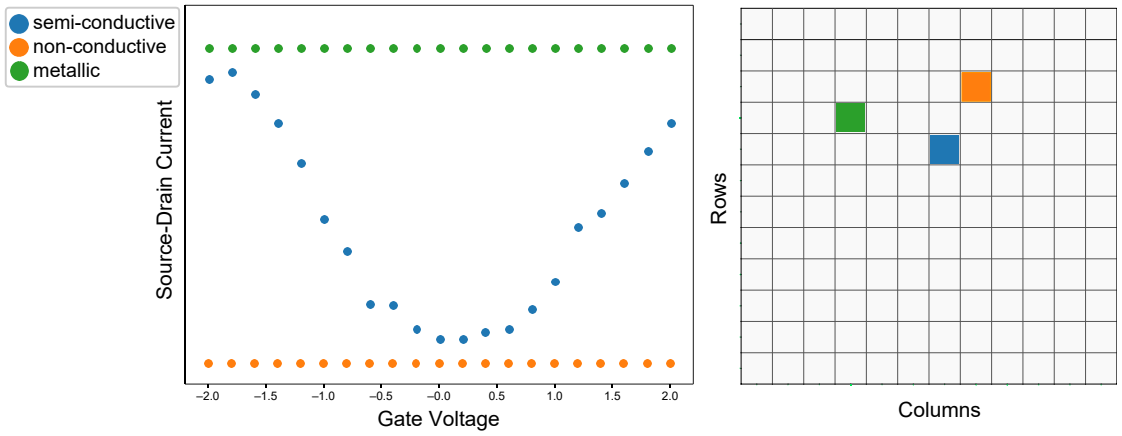

Fig. 5. The left figure shows the measurement of three different types of cells: conductive/metallic (green points), ambipolar semi-conductive (blue points), and non-conductive (orange points). The figure on the right shows the positions of the three characterized cells in the 12×12 matrix of the corresponding daughterboard.

IV. Digital Security Token Production

As explained in the previous section, the motherboard is used to characterize the 144 cells on each daughterboard. Therefore, each cell is selected by switching one row and one column relay on the motherboard using a client-side API that communicates with the Arduino Nano. The cell is then measured by the Keithley 2636B SMU over the GND and I_D connection. A voltage V_{DS} is applied to the remaining not selected cells. A second SMU channel controls the gate voltage V_{GS}. For each cell, the Source-Drain Current I_D is captured for multiple Gate Voltages V_{GS}. The communication with the Arduino Nano, as well as the communication of commands and measurement data with the SMU, are embedded in a test framework, which enables an automated measurement and characterization of all the 144 cells.

After capturing the results, the cells are classified into three different classes: ambipolar semi-conductive, non-conductive, and metallic cells. Semi-conductive cells change their behavior depending on the applied gate voltage; metallic cells and non-conductive cells are, respectively, permanently conductive and non-conductive, independently of the applied gate voltage. This behavior can later be used to generate a robust PUF. Figure 5 shows measurements of three cells on the left side. For the cell corresponding to the blue line, the current changes with the applied gate voltage which makes this cell ambipolar semi-conductive; the green line shows metallic behavior, and the orange one is non-conductive independently of the gate voltage. The right part of the figure shows the identification of the three cells within the relevant 12×12 CNT-FET matrix.

Utilizing these three distinct cases one may create a PUF-based identity in the digital domain by assigning each case to a 2-bit number. In particular, the binary value 11 is assigned to each metallic-behaving cell, the value 00 to each non-conductive, and the value 01 to each semiconducting. This way, each CNT-FET crossbar array has a unique identity of 288 bits (for 144 cells), based on the concatenation of the 2-bit values assigned to each cell based on where it is spatially positioned on the array. Thus, the overall measurement circuitry can provide a digital security token that can be used for security applications in embedded systems and the IoT.

V. Conclusion

In this work, the custom design and implementation of a measurement system suitable for the characterization of nanomaterial-based PUFs, which can be used for security applications in the context of embedded systems and the Internet of Things (IoT), is presented. In particular, the proposed system has been used for the evaluation of CNT-FET crossbar arrays. Our preliminary results validate the proposed methodology, and suggest that the examined framework implementation can also find application in the context of other nanomaterial-based PUFs [3], e.g., PUFs utilising memristor crossbars [4]. Notably, up to now, the swift characterisation and testing of such nanomaterial crossbar structures seemed to require the use of expensive and bulky proprietary devices [5].

References

[1] I. Polian, F. Altmann, T. Arul, C. Boit, R. Brederlow, L. Davi, R. Drechsler, N. Du, T. Eisenbarth, T. Güneysu, S. Hermann, M. Hiller, R. Leupers, F. Merchant, T. Mussenbrock, S. Katzenbeisser, A. Kumar, W. Kunz, T. Mikolajick, V. Pachauri, J.-P. Seifert, F. Sill Torres, and J. Trommer, "Nano Security: From Nano-Electronics to Secure Systems," in *Design, Automation and Test in Europe Conference (DATE). Design, Automation & Test in Europe (DATE-2021), February 1-5, Grenoble, France*, 2 2021, pp. 1334–1339. [Online]. Available: https://doi.org/10.23919/DATE51398.2021.9474187

[2] 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, Jun 2016. [Online]. Available: https://doi.org/10.1038/nnano.2016.1

[3] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "Emerging Physical Unclonable Functions With Nanotechnology," *IEEE Access*, vol. 4, pp. 61–80, 2016. [Online]. Available: https://doi.org/10.1109/ACCESS.2015.2503432

[4] R. Zhang, H. Jiang, Z. R. Wang, P. Lin, Y. Zhuo, D. Holcomb, D. H. Zhang, J. J. Yang, and Q. Xia, "Nanoscale Diffusive Memristor Crossbars as Physical Unclonable Functions," *Nanoscale*, vol. 10, pp. 2721–2726, 2018. [Online]. Available: http://doi.org/10.1039/C7NR06561B

[5] C. Hess, T. Brozek, H. Schneider, Y. Yu, M. Lunenborg, K. H. Ng, D. Ciplickas, R. Vallishayee, C. Dolainsky, and L. H. Weiland, "Evaluation of truly passive crossbar memory arrays on short flow characterization vehicle test chips," in *2019 IEEE 32nd International Conference on Microelectronic Test Structures (ICMTS)*, 2019, pp. 80–84. [Online]. Available: https://doi.org/10.1109/ICMTS.2019.8730984