RRAM Physical Unclonable Functions: Compact Modeling, Array Design, and Optimal Control Schemes for Security Applications

Kamil Ber[1,2], Piotr Wiśniewski[1], Piotr Jeżak[1,2], Aleksander Małkowski[1], Michał Jarosik[1], Adam Pawłowski[1,2], Jakub Ślubowski[1,2], Kacper Sobolewski[1,2], Tomasz Borejko[2], Witold Pleskacz[2]
[1] Centre for Advanced Materials and Technologies CEZAMAT, Warsaw University of Technology, Warsaw, Poland
[2] Institute of Microelectronics and Optoelectronics, Warsaw University of Technology, Warsaw, Poland
e-mails: kamil.ber.dokt@pw.edu.pl; piotr.wisniewski@pw.edu.pl; tomasz.borejko@pw.edu.pl; witold.pleskacz@pw.edu.pl

I. Introduction

The rapid expansion of the Internet of Things has led to the deployment of over 20 billion connected devices [1], ranging from simple home equipment to complex industrial devices. This growth necessitates robust and scalable security solutions that can operate within the constrained power environments typical of battery powered hardware. While traditional cryptographic schemes like AES or RSA are effective, they rely heavily on the secure generation and storage of cryptographic keys, which can be compromised if stored in standard non-volatile memory. Physical Unclonable Functions (PUFs) [2] address these vulnerabilities by serving as hardware security primitives that generate unique, unclonable responses derived from manufacturing process variations. This work focuses on Resistive Random Access Memory (RRAM) [3] as the core component of such a hardware security primitive, leveraging its unique physical properties to create a secure digital fingerprint.

II. RRAM Technology

The RRAM devices utilized in this study consist of a Metal-Insulator-Metal (MIM) structure [3], specifically employing $Al/AlO_x/Pt$ layers fabricated through standard CMOS-compatible processes. These devices are initialized via an electroforming process that induces a soft dielectric breakdown, resulting in the formation of local defects and a conductive filament (CF) that allows current to flow [3]. The device can be switched between a Low Resistance State (LRS) and a High Resistance State (HRS) through *SET* and *RESET* operations, which respectively form or rupture the filament [3]. The intrinsic entropy required for security applications is provided by the stochastic nature of the thermal and ionic mechanisms responsible for these filamentary processes [3]. DC electrical characterization of these fabricated cells was performed to gather empirical data, which was subsequently used to fit parameters for both simple static behavioral models and complex compact electrical models based on Verilog-A.

III. PUF Architecture

The considered PUF architecture employs an RRAM array to serve as a multibit entropy source, with individual cells addressed at the cross points of word and bit lines. Several bit-encoding schemes were evaluated, including bit-wise resistance comparison against a threshold, the use of pristine resistive states in pre-formed cells, and the implementation of parallel or differential RRAM pairs [4]. Analysis indicates that while split-reference schemes offer high density, they are susceptible to environmental drift. Conversely, the pristine state approach offers exceptional robustness and low energy consumption but lacks reconfigurability. This work contends that a differential architecture represents the optimal tradeoff for RRAM-based security applications, as it utilizes both device-to-device and cycle-to-cycle variations while supporting reconfigurability. Simulation of this differential architecture yielded high-quality metrics, specifically achieving a uniformity of 0.5004 and a uniqueness of 0.5002.

IV. Conclusions

This work presents two different methods for RRAM device evaluation in PUF design. The experimental data is used to fit a parameter of a simple static behavioral model and a compact electric model. The behavioral model is used for preliminary evaluation of RRAM technology in security applications, while the compact model will be used for more complex, dynamic evaluation of PUF properties in an analog-mixed signal simulation environment.

Acknowledgment

The research work presented in this paper was carried out within the framework of the FAMES Pilot Line of the Chips JU, funded by Horizon Europe under grant agreement 101182279, Digital Europe under grant agreement 101182297, and Ministry of Science and Higher Education Republic of Poland under Grant Agreement No. MNiSW/2025/DIR/849.

References

[1] S. K. R. Mallidi and R. R. Ramisetty, "Advancements in training and deployment strategies for AI-based intrusion detection systems in IoT: a systematic literature review," *Discov Internet Things*, vol. 5, no. 1, p. 8, Jan. 2025, doi: 10.1007/s43926-025-00099-4.
[2] P. B. Halak, *Physically Unclonable Functions, From Basic Design Principles to Advanced Hardware Security Applications*. Springer, 2018.
[3] H.-S. P. Wong et al., "Metal–Oxide RRAM," *Proc. IEEE*, vol. 100, no. 6, pp. 1951–1970, Jun. 2012, doi: 10.1109/JPROC.2012.2190369.
[4] A. Chen, "Comprehensive assessment of RRAM-based PUF for hardware security applications," in *IEEE International Electron Devices Meeting (IEDM)*, Waszyngton, DC, USA, 2015, pp. 10.4.1–10.4.4.