

# Towards a Reliable PUF Using Organic Thin-Film Transistors

F. de los Santos-Prieto<sup>1</sup>, Deborah Eric<sup>2</sup>, Marc Porti<sup>2</sup>,

R. Castro-Lopez<sup>1</sup>, E. Roca<sup>1</sup>, F. V. Fernandez<sup>1</sup> and Montserrat Nafria<sup>2</sup>

<sup>1</sup>*Instituto de Microelectrónica de Sevilla, IMSE, CNM (CSIC, Universidad de Sevilla), Sevilla, Spain*

\*Corresponding author: fernando@imse-cnm.csic.es

<sup>2</sup>*Departament d'Enginyeria Electrònica, Universitat Autònoma de Barcelona, Bellaterra, Spain*

**Abstract**—As printed electronics continue to evolve, Organic Thin Film Transistors (OTFTs) still present high process-induced variability. Paradoxically, this feature can be used for security purposes. Specifically, Physical Unclonable Functions (PUFs) that provide cryptographic keys for low-cost, resource-constrained applications take advantage of this. However, the reliability of OTFT-based PUFs remains a significant challenge, as thermal annealing, bias stress, and the passage of time (even after being powered off) can introduce instabilities, thus altering the cryptographic keys they generate. To address this issue, we have successfully implemented an optimization-based bit selection approach to enhance their reliability. Our evaluation considers reliability holistically, accounting for thermal annealing, bias stress, and off time degradations. The results demonstrate that by strategically optimizing challenge-response pair selection, the integrity of the generated keys is not compromised. In this work, the feasibility of OTFT-based PUFs and the solutions to key limitations are presented as a step towards improving the practicality and robustness of security solutions for printed electronics.

**Index Terms**—OTFT, PUF, Reliability, Bit Selection, Optimization.

## I. INTRODUCTION

Printing technologies provide several advantages over conventional CMOS transistors. Specifically, organic thin-film transistors (OTFTs) enable the development of low-cost flexible electronics due to their simple fabrication process on plastic substrates [1]. Applications that typically prioritize flexibility and low fabrication costs over computing performance, such as wearable electronics and IoT sensors, are already integrating OTFT as main active devices [2].

Similarly to traditional CMOS circuits, the performance of OTFT-based systems can be enhanced with the inclusion of hardware security blocks, aiming to ensure the security of the device. Physical Unclonable Functions (PUFs) serve as a low-cost solution for generating the cryptographic keys needed in most identification and authentication protocols [3]. While silicon PUFs have been successfully implemented in both academia [4] and industry [5], OTFT-based PUFs remain an emerging field [6]. Advancing these devices could unlock new opportunities in existing and novel applications, such as secure organic sensors and smart packaging, where lightweight, flexible security solutions are in high demand.

PUFs work on the principle of device or circuit parameter variability present in the ICs to create cryptographic keys. This can be due to process variations that happen during the fabrication of the IC, referred to as time-zero variability (TZV), or from time-dependent variability (TDV) that occurs

during the operation of the IC, both of which offer the randomness needed for key generation [7]. Both contribute to the entropy needed for key generation, ensuring each PUF response remains unique and unpredictable, aspects that are crucial for unclonability, as it prevents replication or modeling of the key. However, PUFs must also be reliable, meaning their responses should remain stable despite environmental variations, aging, or operational stress. While OTFTs exhibit sufficient TZV for PUF design, some parameters may provide stronger entropy than others [8]. To develop robust OTFT-based PUFs, it is essential to assess how external factors—such as temperature or bias stress—affect stability, ensuring secure and long-lasting cryptographic implementations in printed electronics [9].

This work analyzes OTFT-based PUFs, using TZV, and examines the impact of said external factors: thermal annealing, bias stress, and off time variations. The proposed PUF concept is based on a differential architecture, where a specific TZV-influenced parameter is compared between two nominally identical elements to generate a bit response. This approach is commonly used in many silicon PUFs, such as those using pairs of ring oscillators [10]. The study examines the TZV of OTFTs by measuring how the device current changes under four different bias conditions to then evaluate whether a PUF can be effectively built using a current comparison between two devices under these same conditions. With this evaluation, the optimal bias condition, based the robustness against TZV, is identified. To further enhance the reliability of the PUF, an optimized transistor pairing strategy is applied, as proposed in [11]. The content of this paper is organized as follows. Section II reviews the OTFT device and evaluates its TZV to implement the OTFT-based PUF. In Section III, the reliability of this PUF is evaluated under the influence of the external factors mentioned above. In Section IV the optimization-based pairing strategy is applied and the results obtained are compared with those presented in the previous section. Section V summarizes and discusses the results.

## II. THE OTFT-BASED PUF CONCEPT

The organic devices used in this study are four-terminal transistors, as shown in Fig. 1. These transistors feature source (S), drain (D), top gate (TG), and back gate (BG) terminals. The devices incorporate gold contacts (G) and the proprietary TRUFLEX material stack, which consists of a base layer (BL), organic semiconductor (OSC), organic gate insulator (OGI), sputter-resistant layer (SRL), and passivation layer (PL). The fabrication process involves sputtering, spin coating, and photolithography. These transistors operate within a nominal voltage range of  $\pm 10$ –30 V. In this study, devices with a channel width (W) of 360  $\mu\text{m}$  and a length (L) of 2.5  $\mu\text{m}$  were characterized.

This work was supported by grant ProyExcel\_00536 funded by Consejería de Universidad, Investigación e Innovación of Junta de Andalucía and by projects PID2022-136949OB-C21 and PID2022-136949OB-C22 funded by MICIU/AEI/10.13039/501100011033 by “ERDF/EU” and by grant USECHIP (TS1-069100-2023-001), project funded by the Secretary of State for Telecommunications and Digital Infrastructure, Ministry for Digital Transformation and Civil Service and by the European Union–NextGenerationEU.

The typical behaviour for the  $I$ - $V$  curves of the devices can be observed in Fig. 2 for a back-gate voltage ( $V_{BG}$ ) of 20 V and four different conditions (fixing  $V_{TG}$  to measure  $I_D$ - $V_D$  or  $V_D$  to measure  $I_D$ - $V_{TG}$ ). In general, the TZV observed in the device's current will depend on the bias point of the transistor. On each device, different  $I$ - $V$  curves have been measured. In particular,  $I_D$ - $V_D$  and  $I_D$ - $V_{TG}$  curves were measured in linear and saturation mode. In both cases, forward (from positive to negative voltages) and backward (from negative to positive voltages) curves were registered. To provide a comprehensive evaluation of the TZV of the device, four different bias points ( $V_{TG}$ ,  $V_D$ ) are considered: (-20V, 5V), (-6V, 5V), (-18V, -1V), and (-20V, -15V) all for a back-gate voltage ( $V_{BG}$ ) of 20 V. These bias points are referred here as linear backward (LB), saturation backward (SB), linear forward (LF), and saturation forward (SF), respectively.

The TZV statistics obtained from 75 different devices for the four cases considered are depicted in Fig. 3. The LB and SF bias points exhibit higher variability compared to the others, with sigma values of 5.6 and 5.5  $\mu$ A, respectively. For a PUF to be practical, selecting an entropy source with high intrinsic variability is crucial. Otherwise, stringent requirements on measurement circuits and techniques become necessary, increasing the complexity of the PUF and affecting its overall performance.

In a differential PUF, a certain parameter is compared between two elements. Each pair of elements constitute a *challenge* while the one-bit comparison result constitutes the PUF's *response*. Ideally, in this pairwise comparison, the distribution of 0s and 1s in the bit responses (also referred as the randomness of the PUF) remains uniform when the two elements are randomly selected. That is, the PUF response should be *unbiased* (i.e., equal proportion of 0s and 1s). Additionally, to prevent information leakage in a differential PUF, each transistor should be used only once in bit generation. That is, each transistor must be paired only once to minimize *bit aliasing*. As a result, before deploying the PUF, the multiple devices in an array must be paired in a specific manner to generate the bit responses.

The architecture of the proposed OTFT-based PUF is depicted in 4a. Two identical transistors, operating under the same bias conditions, are selected by a challenge  $c = \{M_a, M_b\}$  from an array of  $M$  transistors and their currents are compared to obtain a 1-bit response. Although the differential architecture is ideally unbiased, comparisons between

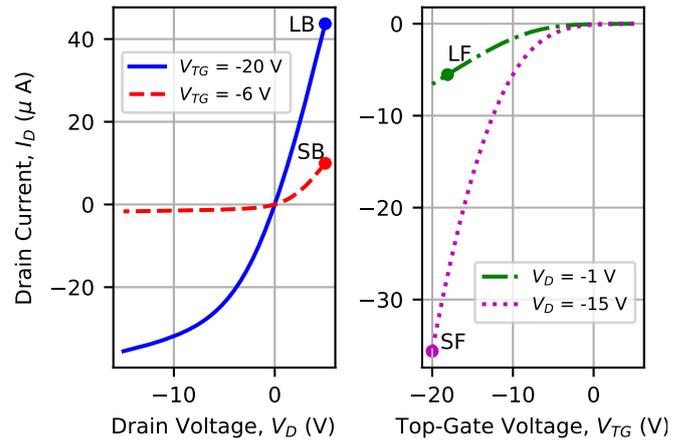


Fig. 2.  $I$ - $V$  curves of an OTFT measured at a back-gate voltage ( $V_{BG}$ ) of 20 V, highlighting the four bias points considered in this work.

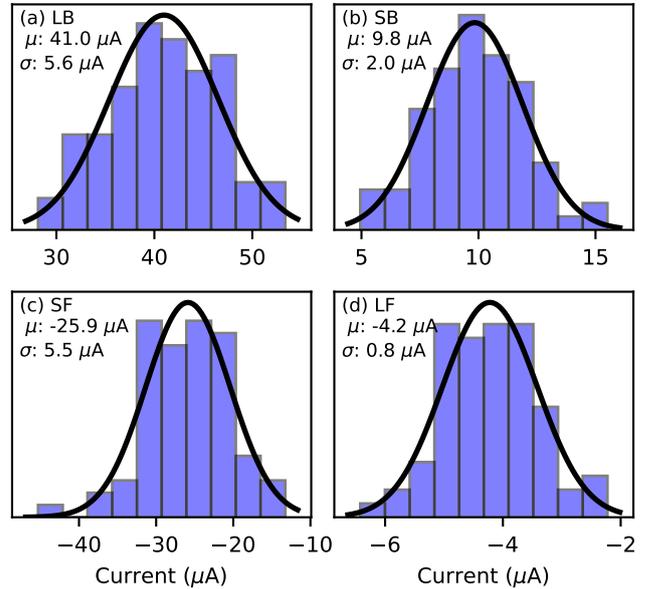


Fig. 3. TZV of device's current at the four bias points considered.

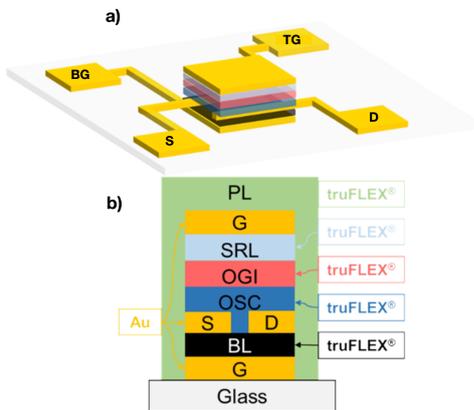


Fig. 1. (a) Three-dimensional sketch of the studied OTFTs where source (S), drain (D), top gate (TG) and back gate (BG) terminals are shown and (b) the device cross-section.

closely matched currents may be systematically assigned to a specific symbol (0 or 1) due to circuit non-idealities (e.g., comparator offsets), potentially degrading the PUF's randomness, as illustrated in Fig. 4b.

To evaluate the performance of the PUF at time-zero, the randomness and the uniqueness, two essential PUF features, are analyzed. Bitstreams of 37 bits are obtained from the 37 possible pairs that can be formed using 75 devices, with 1,000 37-pairs combinations (i.e., 1,000 different PUF instances) used to ensure statistically sound data. Randomness is assessed through the average Hamming Weight ( $HW$ ), while uniqueness (i.e., the PUF's ability to generate distinct responses across different instances) is measured using the average interdie Hamming Distance ( $HD_{inter}$ ) between bitstreams from different pair combinations. To assess the impact of circuit

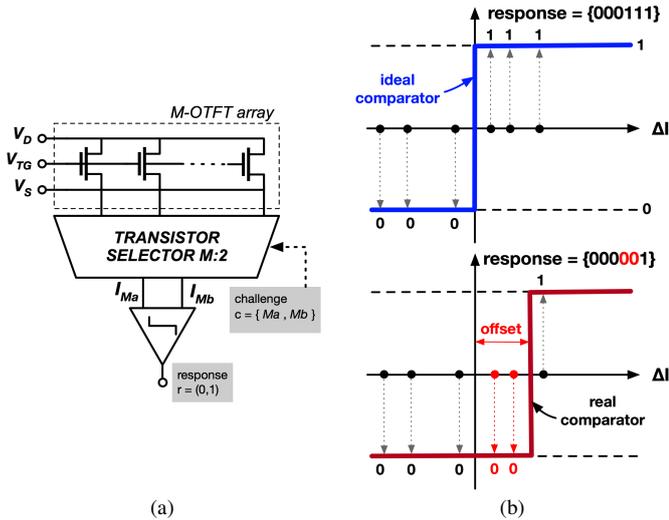


Fig. 4. (a) OTFT-based PUF architecture. (b) Impact of comparator offset.

non-idealities, a comparator offset of  $+0.5 \mu\text{A}$  is introduced<sup>1</sup>. The results are shown in Table I. As expected, the PUF performance improves when OTFTs operate at bias points featuring higher variability (i.e., LB and SF), yielding balanced ( $HW \approx 0.5$ ) and unique ( $HD_{inter} \approx 0.5$ ) bitstreams.

TABLE I  
RANDOMNESS AND UNIQUENESS AT THE FOUR BIAS POINTS.

	LB	SB	SF	LF
$HW$	$0.47 \pm 0.08$	$0.42 \pm 0.08$	$0.47 \pm 0.08$	$0.30 \pm 0.07$
$HD_{inter}$	$0.50 \pm 0.08$	$0.49 \pm 0.08$	$0.50 \pm 0.08$	$0.42 \pm 0.07$

### III. RELIABILITY CONCERNS

Due to the early-stage maturity of printed technologies, various degradation phenomena can affect device performance, leading to bit flips that compromise the reliability of the PUF. This study assesses the impact of three reliability-detrimental effects: off time, bias stress, and thermal annealing [9]. The impact of off time was evaluated by registering the current with a time interval of 1 month. We have also analyzed the behavior of the proposed PUFs after a thermal annealing and after a bias stress. Regarding the thermal annealing, the transistors were subjected to  $50^\circ\text{C}$  for 10 minutes and then cool down until room temperature. The bias stress was evaluated by applying bias values of  $V_{TG} = V_D = -30\text{V}$  ( $V_S = V_{BG} = 0\text{V}$ ) for 5 min to the 75 OTFTs. After each scenario, the responses of the PUF were evaluated and compared to those obtained before.

In Fig. 5, the current shifts induced by each phenomenon are plotted against the respective initial currents for the four bias points considered. Significant positive and negative current shifts are observed, depending on the effect, which can potentially cause bit flips if the two transistors in a pair experience current shifts of differing magnitudes or opposite signs.

The reliability of the PUF under each effect, as well as the combined impact of all effects (denoted as *all*), is evaluated by comparing its responses before and after exposure. The intra-die Hamming Distance,  $HD_{intra}$ , is used as the metric

<sup>1</sup>This offset value has been specifically chosen to evaluate its effect when its magnitude is comparable to the lowest  $\sigma$  among the bias points (LF in Fig.3.d) and when it is an order of magnitude smaller (LB in Fig.3.a).

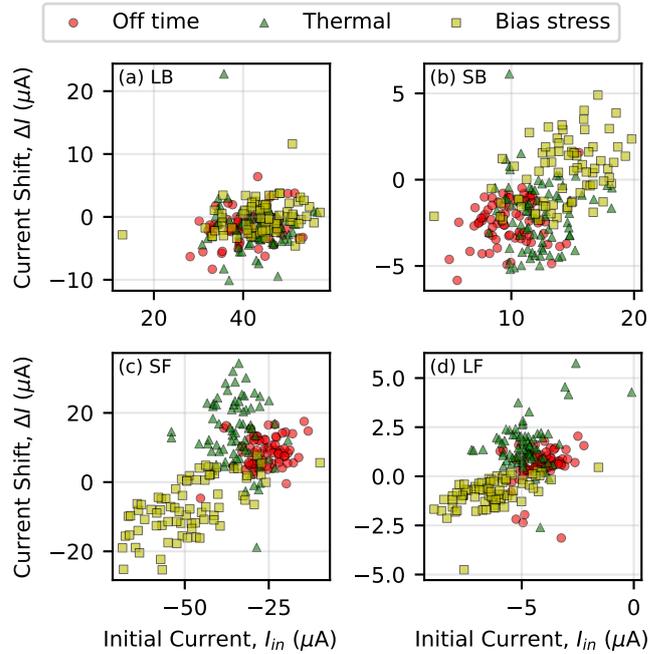


Fig. 5. Current shift caused by each effect against the initial current of the devices.

to quantitatively assess the PUF's reliability ( $Rel$ ), as  $Rel = 1 - HD_{intra}$ . Ideally, the value of  $HD_{intra}$  should be close to 0 ( $Rel \approx 1$ ), as the response bitstream after exposure should remain identical to the initial bitstream. Again, 1,000 different random pair combinations of 37 bits each and a comparator offset of  $0.5 \mu\text{A}$  are used. The  $Rel$  values of the PUF under each effect are shown in Table II, clearly showing that the impact of the different phenomena is quite significant.

TABLE II  
RELIABILITY UNDER EACH EFFECT AT THE FOUR BIAS POINTS.

	LB	SB	SF	LF
<i>off time</i>	$0.87 \pm 0.05$	$0.82 \pm 0.06$	$0.78 \pm 0.06$	$0.78 \pm 0.06$
<i>thermal</i>	$0.87 \pm 0.05$	$0.78 \pm 0.06$	$0.72 \pm 0.07$	$0.75 \pm 0.06$
<i>bias stress</i>	$0.88 \pm 0.05$	$0.79 \pm 0.06$	$0.76 \pm 0.07$	$0.83 \pm 0.06$
<i>all</i>	$0.90 \pm 0.03$	$0.84 \pm 0.04$	$0.81 \pm 0.04$	$0.84 \pm 0.03$

### IV. RELIABILITY ENHANCEMENT THROUGH OPTIMIZATION

Traditionally, two approaches are used to address PUF reliability failures: error-correcting codes (ECCs) and bit selection techniques. While ECCs rely on redundancy to avoid bit flips, bit selection techniques focus on a pre-deployment identification and in-field utilization of the most reliable PUF responses [12].

In this work, to ensure the reliability of the OTFT-based PUF during the in-field application, an evolutionary-based optimized pairing scheme for the devices is proposed, following the approach in [11]. This method leverages the flexibility in forming transistor pairs during the pre-deployment stage to ensure the stability of the responses provided by the selected pairs, thus improving the PUF's lack of reliability shown in Table II.

The optimization problem involves selecting specific pairs of transistors whose currents will be compared to generate the bit responses. Therefore, a candidate solution is defined by the

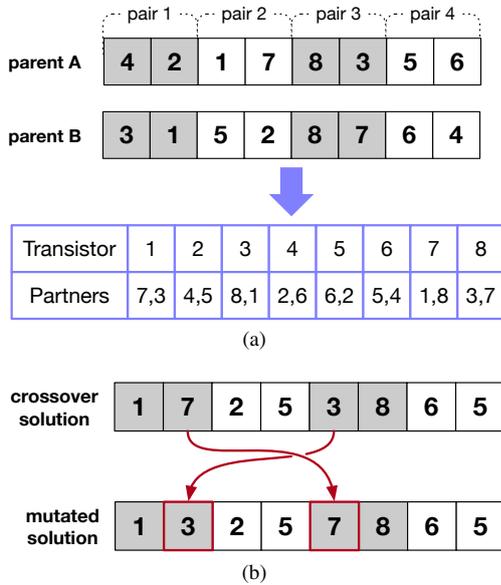


Fig. 6. Proposed operators to obtain new candidate solutions: (a) Crossover table constructed from two previous candidate solutions. (b) Mutation swap.

combination of the available transistor cells in the PUF. In our case, a candidate solution consists of a list of 74 transistors selected from a total of 75, arranged in a specific order. This sorting determines the pairs: for example, the 1st and 2nd transistors in the list form one pair, the 3rd and 4th form another pair, and so on.

In an evolutionary algorithm, a population of candidate solutions (250 in this work) updates and successively improves performance across generations. To ensure the inheritance of key features from selected previous candidate solutions to the next generation, it is crucial to define effective variation operators. These operators, which include crossover and mutation, facilitate the exploration of the solution space while preserving valuable traits from the parent solutions, allowing the algorithm to converge toward optimal or near-optimal solutions efficiently. The crossover and mutation operators, as presented in [11], are depicted in Fig. 6. The crossover is based on the idea that the new candidate solutions should be comprised as far as possible of pairs already present in the previous candidate solutions, while mutation considers swaps between transistors in different pairs according to a mutation rate (0.005 in this work).

Although the optimization algorithm has been shown to enhance the reliability of differential PUFs without compromising their uniqueness and randomness, the incorporation of non-idealities in the comparison, such as offsets, can affect PUF performance. To address this issue, a slight refinement of the fitness function is proposed. An equally weighted sum of the deviations from the ideal values of  $HW$  and  $HD_{intra}$  as  $F = 0.5 \cdot ((1 - |0.5 - HW|) + (1 - HD_{intra}))$  is used to improve the reliability while maintaining the randomness of the PUF.

Table III presents the average reliability results over 10 runs for the optimized population (250 solutions, each one a specific combination of 37 pairs) after the algorithm meets the stopping criterion (defined as 5 consecutive generations without improvement). The statistics shown in this table (average  $\pm$  standard deviation) have been then computed over 2,500 different solutions (i.e., 10 runs of the optimization with 250 solutions each). When compared with the results in Table

II, the improvement has been quite significant. Notably, the LB bias point once again outperforms the other bias points in terms of degradation, achieving near-ideal values regardless of the degradation phenomenon.

TABLE III  
RELIABILITY AT THE FOUR BIAS POINTS AFTER OPTIMIZATION.

	LB	SB	SF	LF
<i>off time</i>	1.00 $\pm$ 0.00	1.00 $\pm$ 0.00	1.00 $\pm$ 0.00	0.97 $\pm$ 0.02
<i>thermal</i>	1.00 $\pm$ 0.00	0.99 $\pm$ 0.01	0.99 $\pm$ 0.01	0.96 $\pm$ 0.02
<i>bias stress</i>	1.00 $\pm$ 0.00	1.00 $\pm$ 0.01	1.00 $\pm$ 0.00	0.99 $\pm$ 0.01
<i>all</i>	1.00 $\pm$ 0.00	0.98 $\pm$ 0.01	0.98 $\pm$ 0.01	0.93 $\pm$ 0.01

## V. CONCLUSIONS

In this work, the feasibility of constructing PUFs using printed technologies such as OTFTs is examined. It is demonstrated that the device's bias point significantly influences the observed current variability. Therefore, properly biasing the devices in the PUF is essential to ensure unbiased bit responses, even in the presence of non-idealities such as offsets. Additionally, a comprehensive reliability study is conducted to assess the PUF's resilience under different degradation effects and to identify the most robust bias point for the transistors. To further enhance reliability and meet the standards of modern applications, an evolutionary-based optimization algorithm is employed for efficient bit selection.

## ACKNOWLEDGMENTS

The OTFT samples were fabricated by SmartKem Ltd. (Manchester, UK) and kindly provided by Eloi Ramón from IMB-CNM (CSIC).

## REFERENCES

- [1] C. Dimitrakopoulos and P. Malenfant, "Organic Thin Film Transistors for Large Area Electronics," *Advanced Materials*, vol. 14, no. 2, pp. 99–117, Jan. 2002.
- [2] M. Kondo *et al.*, "Design of ultraflexible organic differential amplifier circuits for wearable sensor technologies," in *2018 IEEE International Conference on Microelectronic Test Structures (ICMTS)*. Austin, TX: IEEE, Mar. 2018, pp. 79–84.
- [3] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," in *Proceedings of the 44th Annual Design Automation Conference*, ser. DAC '07. New York, NY, USA: Association for Computing Machinery, 2007, p. 9–14.
- [4] A. Santana-Andreo *et al.*, "Reliability improvement of SRAM PUFs based on a detailed experimental study into the stochastic effects of aging," *AEU - International Journal of Electronics and Communications*, vol. 176, p. 155147, Mar. 2024.
- [5] G.-J. Schrijen, "SRAM PUF: The Secure Silicon Fingerprint," <https://www.synopsys.com/designware-ip/security-ip/cryptography-ip/puf.html>, 2024, white Paper.
- [6] M. Porti *et al.*, "On the Aging of OTFTs and Its Impact on PUFs Reliability," *Micromachines*, vol. 15, no. 4, p. 443, Mar. 2024.
- [7] F. De Los Santos-Prieto *et al.*, "A Comprehensive Approach to Improving the Thermal Reliability of RTN-Based PUFs," *IEEE Transactions on Circuits and Systems I: Regular Papers*, pp. 1–0, 2024.
- [8] S. Claramunt *et al.*, "Exploitation of OTFTs variability for PUFs implementation and impact of aging," *Solid-State Electronics*, vol. 207, p. 108698, Sep. 2023.
- [9] H. Matsui, Y. Takeda, and S. Tokito, "Flexible and printed organic transistors: From materials to integrated circuits," *Organic Electronics*, vol. 75, p. 105432, 2019.
- [10] M. C. Martínez-Rodríguez *et al.*, "A Configurable RO-PUF for Securing Embedded Systems Implemented on Programmable Devices," *Electronics*, vol. 10, no. 16, p. 1957, Aug. 2021. [Online]. Available: <https://www.mdpi.com/2079-9292/10/16/1957>
- [11] F. De Los Santos-Prieto *et al.*, "Optimization-based bit selection technique to improve the reliability of PUFs," in *2024 20th International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD)*. Volos, Greece: IEEE, Jul. 2024, pp. 1–4.
- [12] I. Baturone, M. A. Prada-Delgado, and S. Eiroa, "Improved generation of identifiers, secret keys, and random numbers from srams," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2653–2668, 2015.