Experimental Demonstration and Modeling of a Strong PUF Architecture based on Virgin-State Embedded Phase Change Memory

L. Cattaneo, A. Glukhov, P. Mannocci, N. Lepri, J. Jastrzebski, M. Baldo, A. Bonfanti, and D. Ielmini

***Abstract*—Physical Unclonable Functions (PUFs) are essential for lightweight IoT security. While CMOS-based strong PUFs face scalability and unclonability limits, emerging non-volatile memories (NVMs) offer a robust alternative. This work presents the first experimental demonstration of a strong PUF based on virgin-state embedded Phase-Change Memory (PCM). Using a fabricated 90 nm one-transistor/one-resistor (1T1R) PCM test chip, we characterize device behavior over temperature and validate a predictive statistical model. We propose a lightweight masking algorithm to discard unreliable challenge-response pairs (CRPs) with minimal overhead. Results show high entropy, machine-learning resilience, and stable thermal operation at low power, establishing virgin-state PCM as a viable strong PUF technology.**

***Index Terms*—physical unclonable function, hardware security, non-volatile memory, phase change memory, reliability, modeling.**

I. Introduction

Physical Unclonable Functions (PUFs) leverage manufacturing variability to generate unique, unclonable hardware fingerprints for IoT security [1], [2]. Unlike weak PUFs used for key storage, strong PUFs provide a massive challenge-response pair (CRP) space, enabling device authentication without secure non-volatile storage [3], [4]. In this context, the verifier issues a random challenge from the CRP database, and the strong PUF returns its unique response: a match within a tolerance threshold authenticates the device [4].

While CMOS implementations like Arbiter or SRAM PUFs are well-studied, their vulnerability to modeling attacks and limited scalability have motivated the exploration of emerging nonvolatile memories (NVMs), including resistive random access memory (RRAM), magnetoresistive RAM (MRAM), and phase change memory (PCM) [5]. PCM devices are attractive due to their compact footprint and intrinsic stochasticity; however, their reliability under environmental fluctuations remains a critical obstacle for strong PUF applications [4].

In this work, we experimentally demonstrate a strong PUF utilizing the virgin-state of embedded PCM. Using a 90 nm one-transistor/one-resistor (1T1R) PCM test chip, we perform characterization across temperature to calibrate a statistical model for virgin-cell current. To mitigate thermal instability, we introduce a lightweight masking scheme that identifies and discards unreliable CRPs during enrollment.

The paper is structured as follows: Section II describes the PUF architecture and experimental setup; Section III details characterization and model validation; and Section IV discusses performance metrics and reliability strategies.

This work was supported by the EU's Horizon Europe Research and Innovation Programme (Grant 101070679), the ERC (Grant 101069299), and PRIN PNRR 2022 project CAMOUFLAGE (C.U.P. P2022AXCXZ). L. Cattaneo, A. Glukhov, and N. Lepri are now with Innatera Nanosystems B.V., Rijswijk, Netherlands. The work was performed while they were at the Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano and IU.NET, 20133 Milan, Italy, where P. Mannocci, J. Jastrzebski, A. Bonfanti, and D. Ielmini remain (e-mail: daniele.ielmini@polimi.it). M. Baldo is with STMicroelectronics, TR&D, Agrate Brianza, Italy.

II. Strong PUF Design and Experimental Setup

Based on simulations in [6], [7], we designed a test chip in STMicroelectronics 90 nm CMOS technology integrating a 320×128 industry-standard 1T1R array of PCM cells. Utilizing the pristine state avoids programming overhead [8], while Ge-rich $Ge_2Sb_2Te_5$ provides high intrinsic conductance variability, robustness to physical and microscopic analysis, and drift-free stability [6], [7].

The PUF architecture (Fig. 1a) uses a 45-bit shift register to store a 40-bit challenge plus 5 auxiliary bits. To select wordlines (WLs), 30 challenge bits drive five 6-bit decoders addressing disjoint array regions; 5 auxiliary bits independently enable these decoders, forming bitline (BL) current via the aggregate contribution of zero to five selected cells. The remaining 10 challenge bits select a pair of active BLs across four subarrays. Selected BLs are biased at V_{READ} through transimpedance amplifiers (TIAs) with gain R_f. Two rail-to-rail comparators digitize TIA outputs into bits $COMP_{out,0}$ and $COMP_{out,1}$, which are XORed into a 1-bit response. Analog buffers enable direct offset-compensated monitoring of the TIA stages' outputs.

The experimental setup (Fig. 1b) consists of a PCB with a microcontroller and temperature sensors. Thermal characterization involves locally heating the chip (layout in Fig. 1c) with a heat gun, with sensors providing real-time calibration data.

III. PCM Array Characterization and Modeling

The virgin-state PCM array is characterized by measuring TIA output voltages via analog buffers for various V_{READ} and for a variable number of selected cells N:

$$TIA_{out} = V_{READ} + I_{BL}\cdot R_f = V_{READ} + \sum_{i=1}^{N} I_{PCM,i}\cdot R_f, \quad (1)$$

where $I_{PCM,i}$ represents individual cell currents. Experimental current maps for a portion of $Subarray_0$ reveal a unique, stochastic conductance pattern, clearly visible at higher bias (Fig. 2a). The high nonlinearity factor

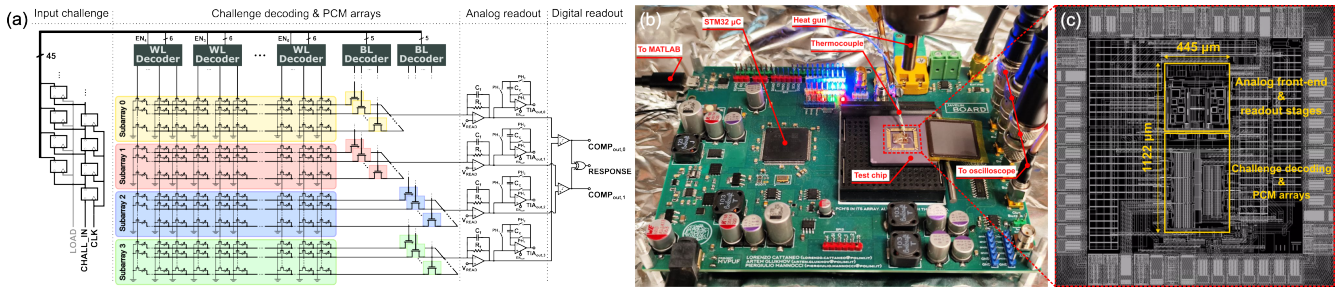

Fig. 1. (a) Schematic of the virgin-state PCM-based strong PUF test chip. A 45-bit input shift register is used to collect the 40-bit challenge and 5 auxiliary bits. The challenge is used for the selection of the active wordlines and bitlines, while the auxiliary bits are used for the actual enabling of the WL decoders. The generated currents are converted into voltages by means of TIA stages, and a random bit is generated by XORing the results obtained from the comparisons of the two pairs of voltages. The output of each TIA stage can be read through a dedicated analog buffer stage. (b) Setup for experimental characterization and testing of the test chip. Printed Circuit Board (PCB) features an STM32 microcontroller to manage the communication interface between the PC and the test chip. Temperature measurements are performed by locally heating the test chip with a heat gun and monitoring the temperature in its immediate vicinity using a type K thermocouple. The outputs of the four TIA stages are read in parallel via an oscilloscope. (c) Global physical layout of the test chip.

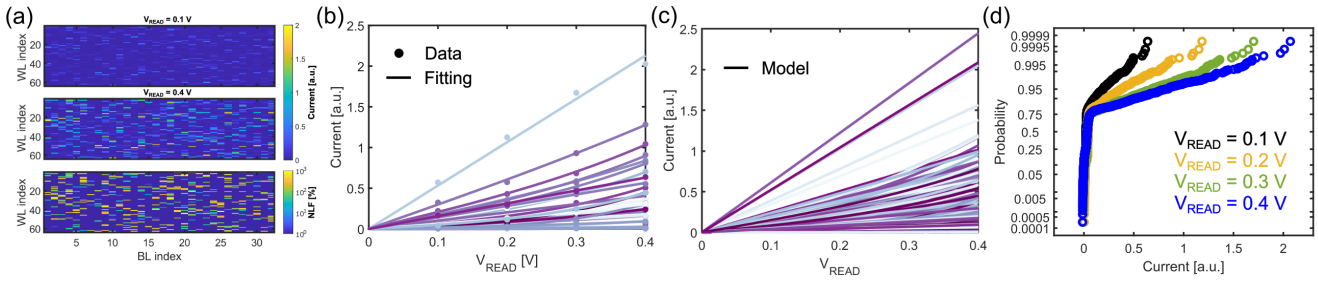

Fig. 2. Characterization of individual cells of Subarray$_0$ at different V_{READ}. (a) Current map for a portion of Subarray$_0$ at $V_{READ} = 0.1V$ and $V_{READ} = 0.4V$, showing random and unpredictable pattern. Nonlinearity factor (NLF) map, highlighting the significant nonlinearity observed between $V_{READ} = 0.1V$ and $V_{READ} = 0.4V$. (b) Experimental IV curves from 35 cells of Subarray$_0$ measured at $V_{READ} = 0.1, 0.2, 0.3, 0.4V$, and associated fitting based on the compact model proposed in [6], [7]. (c) 200 randomly generated IV curves based on the compact model. (d) Current distributions for different V_{READ}. High-resistive cells account for a large part of the distribution.

$NLF = |R_{\text{PCM, 0.1V}}/R_{\text{PCM, 0.4V}} - 1|$ confirms that V_{READ} significantly influences the PUF's operating point, and thus its performance (Fig. 2a). Measured IV curves of individual PCM cells (Fig. 2b) show excellent agreement with the calibrated compact model from [6], [7], allowing for accurate synthetic data generation (Fig. 2c). Notably, only about 25% of the cells provide the primary current contribution (Fig. 2d), suggesting the importance of properly calibrating N.

To address reliability [4], we characterized thermal dependence from 25°C to 85°C. Fig. 3a shows how the virgin-state currents at a fixed read voltage follow the Arrhenius law [9]:

$$I = I_0 \exp\left(-\frac{E_A}{kT}\right), \tag{2}$$

The correlation of 1024 cells between the extracted activation energy E_A and the current at 25°C is reported in Fig. 3b. While E_A typically increases with resistance, the scattering in this correlation is the primary driver of temperature-induced bit-flips. By integrating this experimental scattering into our model, we accurately replicate current distributions across temperatures (Fig. 3c). Finally, measured TIA voltage distributions (Fig. 3d) validate the superposition principle of Eq. (1), with higher V_{READ} and N broadening the available response space. In particular, the distributions can be well approximated by the sum of individual contributions of the selected cells.

IV. Experimental Results

The proposed PUF architecture's challenge length scales as $L = N \cdot \log_2\left(\frac{m}{N}\right) + 2 \cdot \log_2(n)$, where N is the number of selected cells and $m \times n$ is the array size. The CRP space increases exponentially with area, enabling strong PUF [3]. We experimentally calibrate N and V_{READ} to optimize the trade-off between security, entropy, and power.

A. ML resilience and entropy trade-offs

As shown in Fig. 4a, increasing N complexifies the challenge encoding, making the PUF significantly more resilient to predictive ML attacks. At $N = 5$ and $V_{READ} = 0.4V$, the XORed 1-bit responses achieve near-ideal ML resistance regardless of training set size (Fig. 4b). NIST SP 800-22 tests, performed on bitstreams that concatenate 1M of XORed 1-bit responses, confirm that high N and V_{READ} are required to broaden voltage distributions and ensure randomness (Fig. 4c). While higher operating points increase power consumption, they are necessary to provide sufficient entropy for robust authentication. However, the low conductivity of the virgin-state cells results in lower energy consumption than most of the previously proposed solutions (Table I).

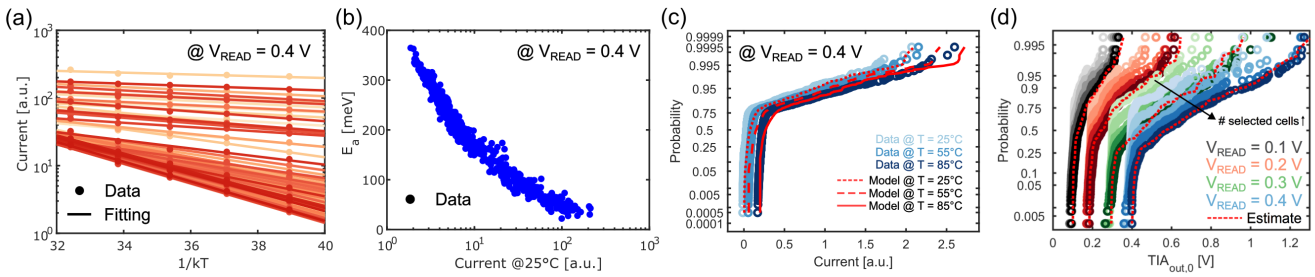

Fig. 3. Temperature measurements of virgin-state PCM cells. (a) Arrhenius behavior of 100 cells at $V_{READ} = 0.4V$, highlighting experimental data and linear fitting. (b) Correlation plot between the activation energy and the current at 25°C, measured at $V_{READ} = 0.4V$. (c) Experimental data and model of current distributions at $V_{READ} = 0.4V$ for different temperatures. (d) Characterization of the TIA stage output. Voltage distribution as a function of the number of selected cells and V_{READ}, with estimated distribution for five selected cells by combining the contributions of the individual cells selected by the challenge.

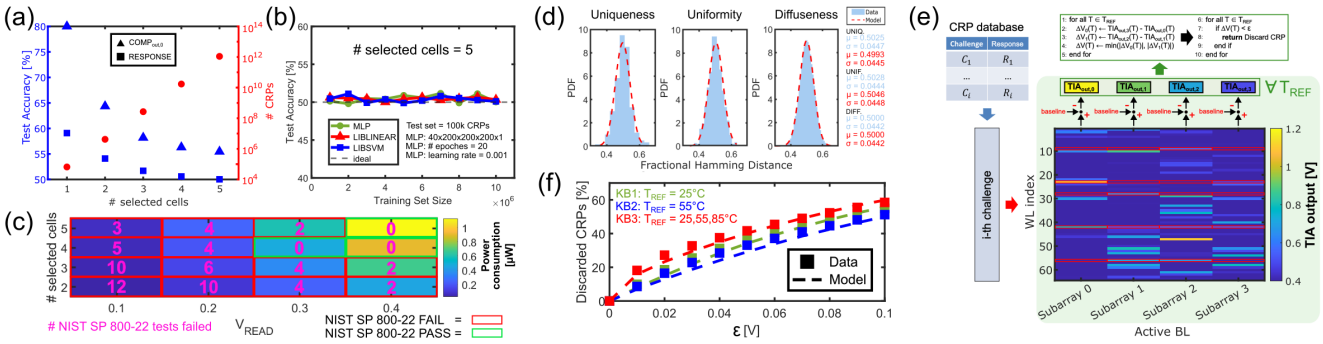

Fig. 4. Experimental results. (a) Number of available CRPs and prediction accuracy of a $L{\times}200{\times}200{\times}200{\times}1$ MLP as a function of selected cells, N. For N = 1, training set was made of 55k CRPs, while for other N it was made of 1M CRPs. Test set was made of 10k/100k CRPs. (b) Prediction accuracy for five selected cells using three different machine learning models, as a function of training set size. (c) Average power consumption of the PUF active area as a function of V_{READ} and the number of selected cells. The number of failed tests of the NIST SP 800-22 standard is reported, evaluated over 55 bitstreams of 18k bits each. The NIST SP 800-22 standard is considered passed if none of its tests fail ($p - value \geq 0.0001$, $bitstream_{passed} \geq 52$) . (d) Uniformity based on 1k 128-bit keys, diffuseness based on 500k comparisons between 128-bit keys, and uniqueness based on 1k 128-bit keys for two PUF instances, at 0.4V. (e) Qualitative representation of the masking algorithm during enrollment. (f) Percentage of discarded CPRs as a function of ε, for different KB schemes.

B. Security metrics

At the optimized operating point ($N = 5$, $V_{READ} = 0.4V$), the PUF demonstrates near-ideal security metrics (Fig. 4d). The response shows near-ideal uniformity ($\mu = 0.5028$, $\sigma = 0.0444$), confirming a balanced ratio of '0's and '1's. Diffuseness ($\mu = 0.5000$, $\sigma = 0.0442$) confirms that each response bit is highly sensitive to variations in the challenge space, ensuring effective intra-device randomness. Finally, the uniqueness across two different instances ($\mu = 0.5025$, $\sigma = 0.0447$) approaches the theoretical 50% Hamming distance (HD), demonstrating strong inter-device discrimination.

C. Lightweight method to improve reliability

To minimize the fraction of bit-flips within a key caused by PCM sensitivity to environmental variations, we extend and experimentally demonstrate the masking methodology originally proposed in [7]. The idea is to evaluate, during enrollment, the minimum absolute voltage difference between the two comparators for a given challenge, denoted as ΔV, and to discard the CRP if ΔV is smaller than a threshold ε. Reliability can be further improved by evaluating ΔV at multiple reference temperatures, and discarding the CRP if at least one measurement does not satisfy the threshold. This prevents unreliable cases where similar compared currents would be prone to flip when temperature changes.

To reduce the enrollment overhead, we leverage the superposition principle (Fig. 3d). With this approach, ΔV can be computed by summing the pre-characterized and baseline-free voltage contributions of individual cells, making it sufficient to map each cell's contribution once at the reference temperatures of interest during enrollment (Fig. 4e). Finally, once unreliable CRPs are flagged, a key-booking (KB) approach [10] associated with the selected reference temperatures can be applied to further maximize reliability. The experimental and predicted percentage of discarded CRPs, for threshold values and key-booking schemes, are shown in Fig. 4f, further highlighting the accuracy of the calibrated model over temperature. The results in terms of bit error rate (BER) for different KB schemes are shown in Fig. 5a-c, where $\varepsilon = 0$ corresponds to the scenario where no masking is applied (native BER). Fig. 5d shows the BER against voltage supply variations, highlighting the benefit of masking for this scenario as well. A comparison with other previously proposed implementations is proposed in Table I.

V. Conclusion

We demonstrated and modeled a low-power strong PUF based on virgin-state PCM, showing its intrinsic random-

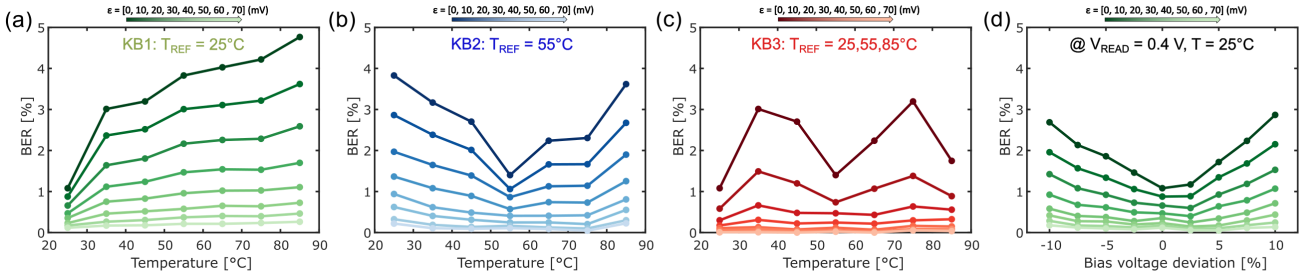

Fig. 5. Reliability for five selected cells and $V_{READ} = 0.4V$. (a) Average BER versus temperature for 128-bit keys, with a single enrollment @25°C. (b) Average BER versus temperature for 128-bit keys, with a single enrollment @55°C. (c) Average BER versus temperature for 128-bit keys, with triple enrollment @25,55,85°C. (d) Average BER versus power supply variation for 128-bit keys.

TABLE I
COMPARISON WITH PREVIOUS CMOS-BASED AND NVM-BASED WORKS

	VLSI '17 [11]	Nature '18 [12]	VLSI '18 [13]	DAC '19 [14]	IEDM '19 [8]	IEDM '21 [15]	IEDM '22 [16]	Nature '25 [17]	This work
Technology	FDSOI 28nm CMOS	Passive ReRAM	Passive ReRAM	55nm LPe CMOS	Passive ReRAM	Passive ReRAM	Passive ReRAM	28nm FeFET	90nm Ge-Rich PCM
PUF Type	Strong	Strong	Strong	Strong	Strong	Strong	Strong	Strong	Strong
Demo Complexity	64 x 64 SRAM ~194 F^2	3D 2 x 10 x 10 ~4 x 4 F^2 0T1R	20 x 20 ~4 x 4 F^2 0T1R	TDM 10 x 10 ~5 x 120 F^2 eFlash	64 x 64 4 F^2 0T1R	8 x 32 2 F^2 4-layer	32 x 32 0T1R	9 x 7 ~1275 F^2 2R1C	320 x 128 ~25 F^2 1T1R
Pre-configuration	Intrinsic	Forming/ Pre-programming	Forming/ Pre-programming	Pre-programming	Pristine State	Pre-programming	Pristine State	Pre-programming	Pristine State
Demo Capacity	$\sim 10^{11}$	$\sim 700 \times 10^6$	$\sim 40 \times 10^6$	$\sim 10^{211}$	$\sim 7 \times 10^{25}$	$\sim 2 \times 10^{12}$	$\sim 10^{17}$	$\sim 10^{77}$	$\sim 10^{12}$
Uncorrected BER	~12.5 % @ 85°C	15 % @ 85°C	4.2 % @ 85°C	~5 % @ 85°C	11.5 % @ 85°C	~1.66 % @ 85°C	~0.9 % @ 80°C	0.7 % @ 85°C	4.76 % @ 85°C
Average Power Consumption / bit	107 μW @ 0.7V	15.9 μW @ 0.3V	21 μW @ 0.3V	~860 μW	0.8 μW @ 0.4V	> 6 μW @ 0.5V	> 128 μW @ 0.2V	Charge-based	1.18 μW @ 0.4V
NIST Test	Not Tested	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
ML Attack	~40 %	~50 %	~50 %	~50 %	~50 %	~50 %	~50 %	~52 %	~50 %

* When not provided, power consumption was estimated based on the median value of the current distribution and the number of cells selected.

ness, entropy, and robustness without programming overhead. Temperature-dependent measurements confirm reproducibility when properly modeled. To improve reliability, we proposed a lightweight CRP filtering scheme enhanced by the statistical model. These results establish virgin-state PCM as a practical and scalable solution for strong PUF implementations.

REFERENCES

[1] R. Carboni and D. Ielmini, "Stochastic memory devices for security and computing," *Advanced Electronic Materials*, vol. 5, no. 9, p. 1900198, 2019.

[2] A. Shamsoshoara, A. Korenda, F. Afghah, and S. Zeadally, "A survey on physical unclonable function (puf)-based security solutions for internet of things," *Computer Networks*, vol. 183, p. 107593, 2020.

[3] F. Zerrouki, S. Ouchani, and H. Bouarfa, "A survey on silicon pufs," *Journal of Systems Architecture*, vol. 127, p. 102514, 2022.

[4] M. Mahmoodi, D. Strukov, and O. Kavehei, "Experimental demonstrations of security primitives with nonvolatile memories," *IEEE Transactions on Electron Devices*, vol. 66, no. 12, pp. 5050–5059, 2019.

[5] 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, 2017.

[6] L. Cattaneo, M. Baldo, N. Lepri, F. Sancandi, M. Borghi, E. Petroni, A. Serafini, R. Annunziata, A. Redaelli, and D. Ielmini, "Enhancing reliability of a strong physical unclonable function (PUF) solution based on virgin-state phase change memory (PCM)," in *2023 IEEE International Reliability Physics Symposium (IRPS)*. IEEE, 2023, pp. 1–6.

[7] L. Cattaneo and D. Ielmini, "A strong physical unclonable function with virgin state embedded phase change memory," *IEEE Transactions on Electron Devices*, 2024.

[8] M. Mahmoodi, H. Nili, Z. Fahimi, S. Larimian, H. Kim, and D. Strukov, "Ultra-low power physical unclonable function with nonlinear fixed-resistance crossbar circuits," in *2019 IEEE International Electron Devices Meeting (IEDM)*. IEEE, 2019, pp. 30–1.

[9] M. Baldo, O. Melnic, M. Scudieri, G. Nicotra, M. Borghi, E. Petroni, A. Motta, P. Zuliani, L. Laurin, A. Redaelli *et al.*, "Modeling and analysis of virgin ge-rich gst embedded phase change memories," *IEEE Transactions on Electron Devices*, vol. 70, no. 3, pp. 1055–1060, 2023.

[10] M. R. Mahmoodi, Z. Fahimi, S. Larimian, H. Nili, H. Kim, and D. B. Strukov, "A strong physically unclonable function with $>2^{80}$ CRPs and $<1.4\%$ ber using passive ReRAM technology," *IEEE Solid-State Circuits Letters*, vol. 3, pp. 182–185, 2020.

[11] S. Jeloka, K. Yang, M. Orshansky, D. Sylvester, and D. Blaauw, "A sequence dependent challenge-response puf using 28nm sram 6t bit cell," in *2017 Symposium on VLSI Circuits*. IEEE, 2017, pp. C270–C271.

[12] H. Nili, G. C. Adam, B. Hoskins, M. Prezioso, J. Kim, M. R. Mahmoodi, F. M. Bayat, O. Kavehei, and D. B. Strukov, "Hardware-intrinsic security primitives enabled by analogue state and nonlinear conductance variations in integrated memristors," *Nature Electronics*, vol. 1, no. 3, pp. 197–202, 2018.

[13] M. R. Mahmoodi, H. Nili, and D. B. Strukov, "Rx-puf: Low power, dense, reliable, and resilient physically unclonable functions based on analog passive rram crossbar arrays," in *2018 IEEE Symposium on VLSI Technology*. IEEE, 2018, pp. 99–100.

[14] M. Mahmoodi, H. Nili, S. Larimian, X. Guo, and D. Strukov, "Chipsecure: A reconfigurable analog eflash-based puf with machine learning attack resiliency in 55nm cmos," in *Proceedings of the 56th Annual Design Automation Conference 2019*, 2019, pp. 1–6.

[15] Q. Ding, H. Jiang, J. Li, C. Liu, J. Yu, P. Chen, Y. Zhao, Y. Ding, T. Gong, J. Yang *et al.*, "Unified 0.75 pj/bit trng and attack resilient 2f 2/bit puf for robust hardware security solutions with 4-layer stacking 3d nbo x threshold switching array," in *2021 IEEE International Electron Devices Meeting (IEDM)*. IEEE, 2021, pp. 39–2.

[16] J. Park, T.-H. Kim, S. Kim, M. S. Song, S. Youn, K. Hong, B.-G. Park, and H. Kim, "Highly reliable physical unclonable functions using memristor crossbar with tunneling conduction," in *2022 International Electron Devices Meeting (IEDM)*. IEEE, 2022, pp. 18–3.

[17] T. Li, X. Guo, F. Müller, S. Abdulazhanov, X. Ma, H. Zhong, Y. Liu, V. Narayanan, H. Yang, K. Ni *et al.*, "Demonstration of high-reconfigurability and low-power strong physical unclonable function empowered by fefet cycle-to-cycle variation and charge-domain computing," *Nature communications*, vol. 16, no. 1, p. 189, 2025.