A Strong Physical Unclonable Function With Virgin State Embedded Phase Change Memory

L. Cattaneo, *Graduate Student Member, IEEE and D. Ielmini, Fellow, IEEE*.

***Abstract*— Physical unclonable functions (PUFs) have gained attention in recent years due to the increasing demand for secure, compact, and power-efficient electronic devices in the Internet of Things (IoT). PUFs can provide a unique physical fingerprint to each device, which is a valuable means of enhancing security through the generation of unique and volatile cryptographic keys with no need to store them in non-volatile memory. A major concern regarding PUF solutions for low-cost authentication is achieving robustness, a large challenge-response pair (CRP) space, and high reliability against environmental variations at the same time. In this work, we present a PUF system based on embedded phase change memory (PCM) in the virgin state with industry-standard one-transistor/one-resistor (1T1R) cell, exploiting the wide resistance distribution as an entropy source. The PUF system is validated based on extensive physics-based simulations of embedded PCM cells integrated in 90 nm technology, showing raw reliability in temperature comparable with state-of-the-art solutions which can be further improved using dedicated schemes for the selection of reliable CRPs.**

***Index Terms*— physical unclonable function (PUF), phase change memory (PCM), non-volatile memory (NVM), reliability modeling, hardware security**

I. Introduction

The widespread diffusion of the Internet of Things (IoT) and the growing need to ensure the secure transfer and authentication of data have led to the development of reliable cryptographic solutions and hardware primitives in recent years [1], [2]. While typical systems rely on keys explicitly stored in non-volatile memories (NVMs), which is prone to the risk of physical and side-channeling attacks [3], physical unclonable functions are gaining interest as low-cost and energy-efficient alternatives for generating volatile keys on demand [4].

The physical unclonable function (PUF) is a system that statistically maps an input digital word (challenge) into an output response, based on intrinsic and unique properties acting as entropy sources (Fig. 1). Each challenge-response pair generated defines a CRP, and depending on the number of CRPs, different PUF applications can be enabled. One of the most popular PUF applications is lightweight authentication, for which a low-cost protocol consisting of an enrollment and a verification phase is required. During the initial enrollment phase, a certain number of CRPs are tested in a trusted environment and recorded in a database, while during the verification phase, a set of challenges is provided to the PUF system in an untrusted environment and the corresponding responses are compared with the expected ones. PUF systems suitable for this type of application are called strong PUFs, for which a large CRP space and robustness to mathematical modeling are required, although they are typically more susceptible to environmental variations [4]. In this scenario, achieving high reliability while guaranteeing all other properties is a complex task, which is increasingly being tackled by resorting to solutions based on emerging non-volatile memories. One of the most interesting emerging memory technologies for the implementation of NVM-based PUF is phase change memory (PCM), both for its intrinsically stochastic properties [5], [6] and its already demonstrated scaling to advanced technology nodes [7], [8].

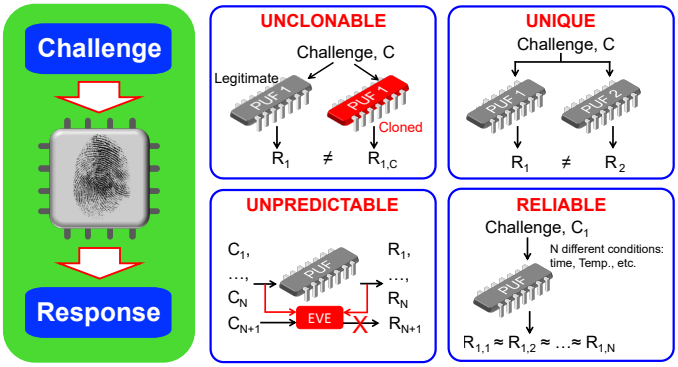


Fig. 1. Summary of primary properties of a physical unclonable function. To be effective in enhancing the security of hardware systems, a PUF must exhibit physical and mathematical unclonability, as well as unique, unpredictable, and reliable responses.

This work proposes an extension of the strong PUF concept based on industry-standard one-transistor/one-resistor (1T1R) embedded PCM in the virgin state presented in [9]. The main novel contributions consist of: (i) a description of the compact modeling of the 1T1R cell, (ii) an analysis of the effects of the array's physical dimensions over the entropy, (iii) an analysis of the effects of V_{READ} and V_{GS} over entropy, current distributions and power consumption, and (iv) a detailed analysis on the impact of temperature and voltage variations on the architecture.

This project has received funding from the European Research Council (ERC) under grant agreement no. 101069299. L. Cattaneo and D. Ielmini are with the Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano and IU.NET, 20133 Milan, Italy (e-mail: daniele.ielmini@polimi.it).

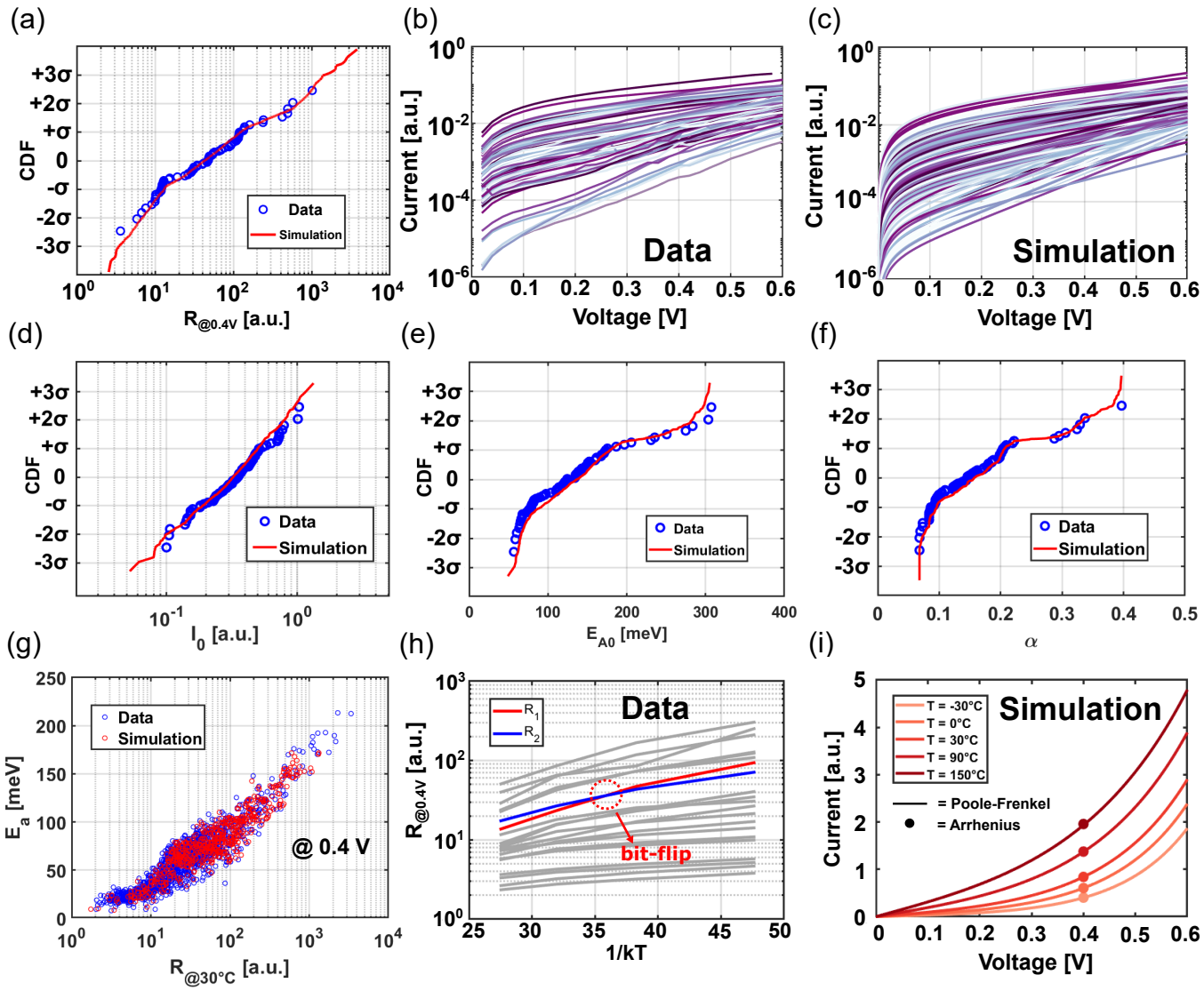


Fig. 2. (a) Resistance distribution of Ge-rich PCM cells in the virgin state, fabricated in the 90 nm technology node. Model fitting covers 3 decades, according to [11]. Measured at 0.4 V. (b) Measured I-V characteristics from 72 virgin PCM cells. (c) 200 randomly generated I-V curves based on our model. (d) Distribution of I_0 parameters, extracted from 72 experimentally measured curves, and from 1k simulated I-V characteristics. (e) Distribution of E_{A0} parameters, extracted from 72 experimentally measured curves, and from 1k simulated I-V characteristics. (f) Distribution of α parameters, extracted from 72 experimentally measured curves, and from 1k simulated I-V characteristics. (g) Experimental and simulated correlation plot between the activation energy E_A and resistance R at 0.4V of PCM cells, where R is measured at 30℃. (h) Temperature variability. Arrhenius of 20 PCM cells experimentally measured at different temperatures. When the Arrhenius behaviors of two cells cross each other, a bit-flip may occur from that temperature onwards [11]. (i) I-V characteristic of a simulated PCM cell for T = -30, 0, 30, 90, 150 ℃ based on the proposed model. The dots represent the expected currents based on the Arrhenius law in Eq. 6 considering the same resistance value R at 0.4 V and the same activation energy value E_A at 0.4 V used to extract the entire I-V curve.

II. Modeling of Virgin-State PCM Devices

The use of embedded memory devices in the virgin state has already been proposed to simplify the peripheral circuitry of PUF systems, avoiding the overhead necessary for programming [10]. In this scenario, embedded PCM with Ge-rich $Ge_2Sb_2Te_5$ (GST) in the pristine state appears an optimal candidate for PUF implementations thanks to its intrinsic wide conductance variability and robustness to invasive Scanning Transmission Electron Microscopy (STEM) analysis [9], [11]. Another crucial feature is the absence of temporal drift, since after deposition the GST is exposed to very high-temperature treatments during BEOL integration such as metal and oxide deposition [12]. During these treatments the eventual complete crystallization takes place, reaching a fully-evolved state that makes it immune to further changes for any subsequent bake. On the other hand, the temperature-dependent conductivity of the PCM cells makes the current-based responses easily affected by environmental variations [11], affecting the reliability of the PUF.

The modeling of virgin-state PCM devices for this study is based on the experimental data of I-V curves and the temperature behavior of a subset of cells measured within the same array. Fig. 2a shows the wide resistance distribution of the virgin state measured at 0.4 V and T = 30 °C, due to

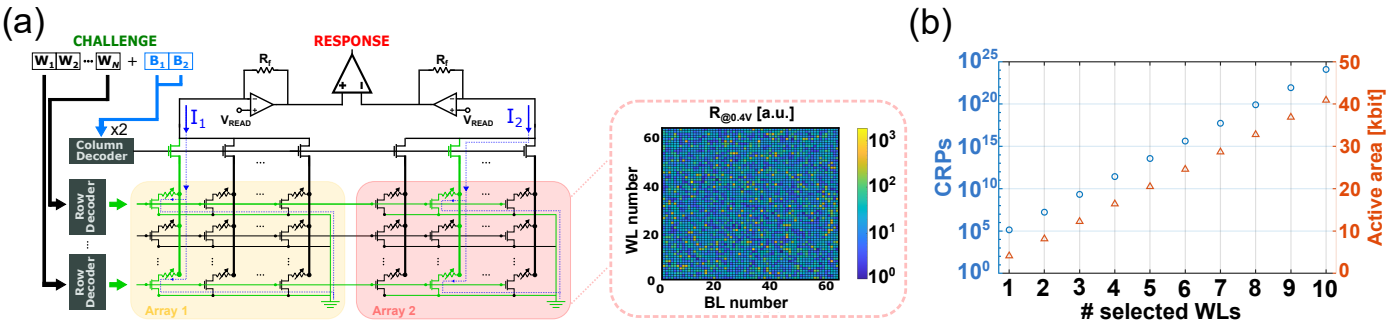


Fig. 3. (a) Array pair and comparison principle. In each array, an input challenge selects *N* wordlines and one bitline, generating a current I_j given by the sum of *N* cells. The selection of each WL is managed by a dedicated row decoder, addressed by the portion W_i of the input challenge, with *i* from 1 to *N*. The two currents of the two arrays are compared to generate a response bit. In the figure, an example map of cell's resistances (a.u.) in a 64x64 array measured at 0.4 V is proposed. (b) Challenge-response pair (CRP) space and corresponding active area per array required for implementation, considering $\frac{m}{N}$ = 128 and 32 bitlines (n = 32).

the presence of Ge grains as a result of segregation in the poly-crystalline material [11]. The I-V curves of the virgin state PCM shown in Fig. 2b were modeled assuming a Poole-Frenkel model [13]:

$$I = I_0 \exp\left(-\frac{E_{A0}}{kT}\right) \sinh\left(\alpha \frac{qV}{kT}\right) \tag{1}$$

Fig. 2c shows the simulated I-V curves for 90 nm embedded virgin state PCM devices, showing good accordance between data and our model. To generate an I-V curve, a random resistance value R read at 0.4 V is firstly extracted from the lognormal distribution that best fits the experimental data in Fig. 2a, at T = 30°C. Then, the parameters a and b are computed for the simplified curve expression:

$$I = \sinh(a \cdot V) \ \exp(b) \tag{2}$$

where the computation is based on the experimental correlations between a, b, and R. The parameters I_0, E_{A0} and α of Eq. (1) in Fig. 2d-f are then derived from the parameters a, b, and the activation energy E_A measured at 0.4 V correlated with R in Fig. 2g, using the following equations [13]–[15]:

$$a = \alpha \frac{q}{k_B T} \tag{3}$$

$$E_A = E_{A0} - qV\alpha \cdot \coth\left(\alpha \frac{qV}{k_B T}\right) \tag{4}$$

$$b = \log(I_0) - \frac{E_{A0}}{k_B T} \tag{5}$$

The temperature dependence of the I-V curves is extracted based on the temperature dependence of the parameters a and b. As reported in [11] and shown in Fig. 2h, the pristine PCM cell resistance shows an Arrhenius behavior for the reading voltage 0.4 V:

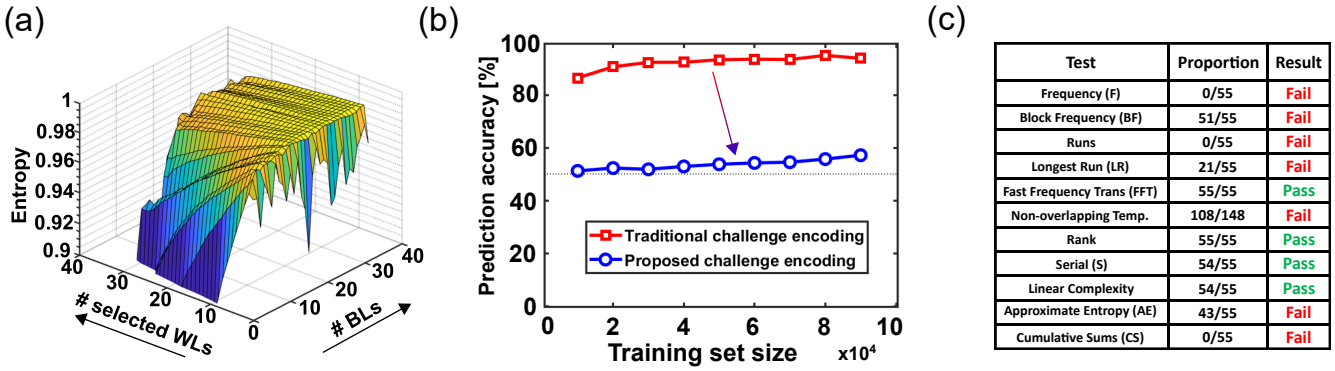
$$R = R_0 \exp\left(\frac{E_A}{kT}\right) \tag{6}$$

The expected behavior is well represented by our model, as shown in Fig. 2i.

III. PCM-BASED STRONG PUF CONCEPT

The wide and random resistance distribution of the virgin state can be exploited as an entropy source to generate unique fingerprints from each array. Fig. 3a shows the basic block for the strong PUF architecture, consisting of two 1T1R arrays of size $m \times n$ addressed in parallel by an input challenge. The challenge is split into two segments: the first one encodes the addresses of *N* rows, which are provided to *N* row decoders responsible for the selection of one row (wordline, WL) out of $\frac{m}{N}$ each, while the second one encodes the addresses of two columns (bitlines, BLs), one per array. Two bitline currents $I_j = \sum_{i=1}^{N} G_{i,j} V_j$ are generated according to the vector-vector multiplication (VVM) concept [16], where $G_{i,j}$ are the conductances at the *j*th bitline and V_j the applied voltage, and compared to yield a random response bit. The PUF thus requires $L = N \times log_2\left(\frac{m}{N}\right) + 2 \times log_2(n)$ challenge bits to generate a single-bit response. Fig. 3b shows the number of CRPs and the active area of one array as a function of the number *N* of selected WLs: modifying *N* affects the length of the challenge, ensuring an exponential increase of the CRP space equal to 2^L with the linear increase of the active area and enabling strong PUF [4].

Fig. 4a shows the average Shannon's entropy of bitstreams created concatenating several responses to sequential input challenges as a function of the physical dimensions of the array (the number of BLs) and the number of selected WLs. To maximize entropy the number of physical BLs should be maximized, with only a few selected WLs to prevent excessive averaging and power consumption. At the same time, the number of WLs should not be too low to avoid falling into a simple bias-inducing cell-wise comparison. Fig. 4b compares the robustness against machine learning (ML) attacks encoding the challenge in two different ways, namely (i) directly applying the challenge's bits as electrical signals to rows and columns as done in [17], and (ii) using the proposed approach. The latter ensures a more uniform challenge in terms of balance between 0s and 1s enhancing robustness due to a more complex mapping. On the other hand, the simple implementation of Fig. 3a cannot provide sufficient entropy, as evidenced by the insufficient resilience to ML attacks in Fig. 4b and NIST Test failure in Fig. 4c.



Test	Proportion	Result
Frequency (F)	0/55	Fail
Block Frequency (BF)	51/55	Fail
Runs	0/55	Fail
Longest Run (LR)	21/55	Fail
Fast Frequency Trans (FFT)	55/55	Pass
Non-overlapping Temp.	108/148	Fail
Rank	55/55	Pass
Serial (S)	54/55	Pass
Linear Complexity	54/55	Pass
Approximate Entropy (AE)	43/55	Fail
Cumulative Sums (CS)	0/55	Fail

Fig. 4. (a) Average Shannon's entropy of the bitstream obtained concatenating responses generated by the array pair architecture, considering m = 32. Shannon's entropy is used to measure the ratio of '0' bits to '1' bits. A Shannon's entropy equal to 1 indicates a random bitstream with 50% probability that each selected bit is '0' or '1', while a Shannon's entropy of less than 1 indicates a bias towards '0' or '1'. (b) Comparison of resilience against a machine learning attack using two different challenge encodings with equal challenge length and number of selected cells. Traditional encoding directly applies the challenge as electrical signals to WLs and BLs for selection. Here, the proposed encoding is more robust, but accuracy still increases with training set size. (c) NIST Test result based on 55 bitstreams of 232k-bit each. Since more than one statistical test failed, the NIST Test as a whole gives a negative result.

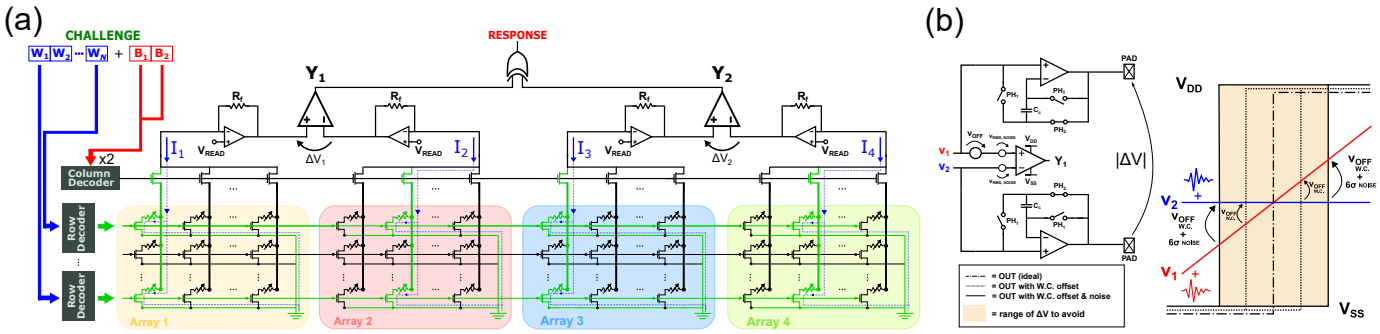


Fig. 5. (a) PUF architecture. Two pairs of $m \times n$ arrays are addressed in parallel with the same challenge, which selects *N* WLs through *N* row decoders and a combination of two active BLs, the same for both pairs. The resulting bits (Y_1 and Y_2) serve as input to an XOR gate, which generates the response. The architecture allows the separate reading of the two voltage differences ΔV_1 and ΔV_2 at the input of the comparators to manage the CRP selection scheme. When the scheme is enabled, a challenge is discarded if either voltage difference is below a certain threshold, chosen according to the expected noise and offset contributions. (b) Circuitry for the reading of the voltage difference between two voltages v_1 and v_2. An offset-compensated analog buffer is used after each TIA stage to read the voltage values at the comparator's inputs. The input-referred offset of the comparator and the noise superimposed on the signal could affect the comparison.

IV. PUF Design and Result Discussion

A. PUF architecture and CRP selection scheme

Fig. 5a shows the entire PUF architecture, consisting of two pairs of 1T1R arrays of size $m \times n$ each similar to the core in Fig. 3a. The input challenge is presented to both pairs according to the same principle explained in Section III thus generating two random bits Y_1 and Y_2. A transimpedance amplifier (TIA) with gain R_f converts each current to a voltage value, while the comparison is performed by a rail-to-rail voltage comparator. The final response is generated by XORing the output bits to increase the entropy of the bitstream [18]. The voltages at the input of the comparators can be separately read using offset-compensated analog buffers, to enable the proposed CRP selection scheme. In particular, if a challenge yields a voltage difference $|\Delta V_{1,2}| < \varepsilon$, then the challenge is discarded. The threshold value ε is defined based on the expected contributions of noise at the input nodes of the comparators and offset of the comparator. These contributions are extracted from simulations performed on readout chain design implemented in Cadence Virtuoso, using a 90 nm technology commercial PDK. To evaluate the impact of the expected noise at the output of the TIA, several Monte Carlo simulations were performed over a set of transient noise runs in a real-case scenario, to define the distribution of the root mean square (RMS) noise contribution, which represents the standard deviation of the noise superimposed on the signal. On the other hand, to assess the value of the offset referred to the input of the comparators, which is modeled in series with the non-inverting input, several Monte Carlo simulations were performed under different conditions of the inverting input to extract systematic and statistical contributions.

As shown in Fig. 5b, similar currents could lead on one side to biased comparisons affected by the offset of the comparator, and on the other to unreliable responses affected by the noise superimposed on the signal. Thus, discarding CRPs associated with comparisons of similar currents helps to improve the uniformity, and to reduce the overall probability of bit-flip events [9]. The number of CRPs discarded at a certain threshold value ε depends on the distribution of the compared currents and the gain R_f of the TIA stage.

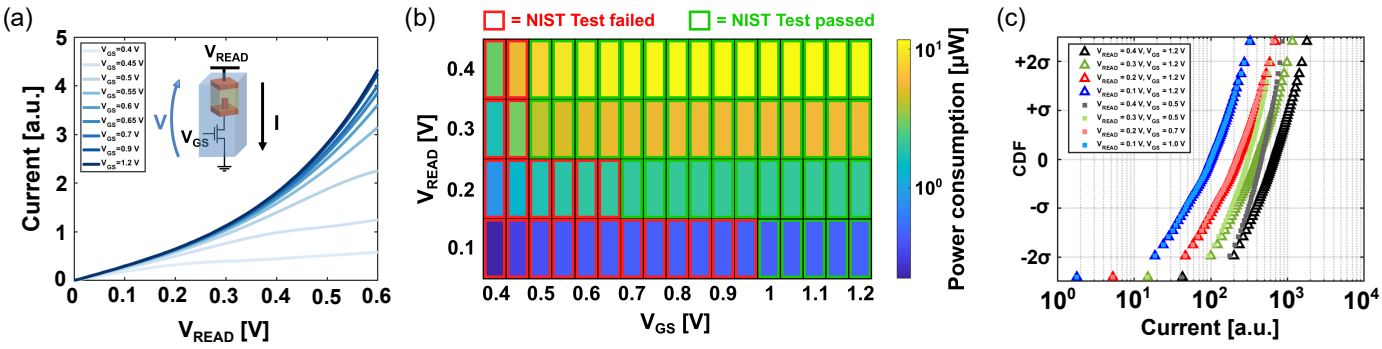


Fig. 6. (a) I-V curve of a simulated 1T1R cell, varying the gate voltage V_{GS}. The x-axis represents the voltage V_{READ} imposed on the top electrode. (b) NIST Test passing and power consumption of the active area for $N = 5$ as a function of V_{GS} and V_{READ}. Evaluated based on the tests shown in Fig. 4c for 55 bitstreams of 23k-bit each. The NIST Test is passed if none of its statistical tests fail. (c) Current distributions for 5 selected cells, considering the minimum and maximum V_{GS} allowed at various V_{READ}.

B. Entropy-power trade-off

The MOSFET selector in a 1T1R cell adds a degree of freedom to the PUF operation, namely the gate voltage V_{GS} modulation. Fig. 6a shows the I-V characteristic of a simulated 1T1R cell as a function of the applied top electrode and gate voltage, highlighting a significant modification of the curve depending on the applied V_{GS} at higher voltages. These results show that relatively small V_{GS} can still ensure enough entropy for the generation of the response while allowing reduced power consumption. This is shown in Fig. 6b, where the entropy and the power consumption for $N = 5$ selected cells are reported as a function of the applied V_{READ} and V_{GS}. In particular, to quantify the entropy of the bitstream obtained by the concatenation of responses to various challenges we used the NIST SP 800-22 Test Suite [19], considering the outcome valid only in case each one of its statistical tests is passed. For this study, the applied V_{READ} was limited to 0.4 V to avoid possible unwanted programming of the virgin-state cell during the reading phase. The results show that specific combinations of V_{READ} and V_{GS} are enough to guarantee sufficient entropy thus reducing energy consumption. Fig. 6c shows the modulation of the current distributions for the minimum and maximum allowed V_{GS} at various V_{READ}, with $N = 5$ selected cells. If V_{GS} is further reduced, the voltage drop across the PCM resistance decreases in the 1T1R structure, thus resulting in narrower current distributions and a decrease of the PUF entropy. In order to enable the comparison of currents that may vary significantly depending on the chosen combination of V_{READ} and V_{GS}, the gain R_f of the TIA stage must be calibrated accordingly to match the comparator's rail-to-rail input range, also considering the modulations of the current distribution due to temperature. Considering $V_{READ} = 0.4$ V, $V_{GS} = 1.2$ V and a gain $R_f = 20\text{k}\Omega$, our PUF shows nearly ideal statistical properties in terms of diffuseness ($\mu = 50.00\%$, $\sigma = 4.42\%$), uniqueness ($\mu = 50.00\%$, $\sigma = 4.41\%$), and uniformity ($\mu = 49.99\%$, $\sigma = 4.42\%$) for 128-bit keys.

C. Reliability against environmental variations

Referring to temperature variations, the current dependence of PCM cells and MOSFETs on temperature could lead to an error when environmental conditions change since the response is generated based on a current comparison (Fig. 2h). This effect can be quantified with the bit error rate (BER), namely the percentage of bit-flips occurring within a key by changing the operating temperature. Solutions already proposed to mitigate the impact of temperature variations consist of (i) dismissing unstable bits [10] and (ii) adopting key-booking schemes [20]. In particular, key-booking means that one or multiple enrollments are carried out at various reference temperatures, and the response obtained on the field is compared with the corresponding CRP of the dataset at the closest temperature to the chip. Our solution combines these two approaches by adapting the CRP selection scheme to the chosen reference temperatures.

Two different contributions can influence BER, namely (i) the noise and (ii) the read current dependence on the temperature. The first is relevant whenever the compared currents are similar, while the second is relevant in case the different T-dependent variations of the currents yield an opposite response. Fig. 7a shows the average BER at T = 85°C and the percentage of discarded CRPs as a function of the chosen threshold ε for $V_{READ} = 0.4$ V and two different V_{GS} conditions. For $\varepsilon = 0$, we find the raw BER since no selection of CRPs is applied, whereas increasing ε means reducing BER at the cost of more discarded CRPs. Interestingly, the raw BER appears slightly better for smaller V_{GS}. Avoiding the comparison of similar currents at T_{ref} results in both the mitigation of the noise effect around the reference and the reduction of the overall probability of crossing currents at different temperatures. The latter depends on the PCM and MOSFET technology parameters and can be quantified.

Given two different temperatures T_{ref} and T_{read} with $T_{ref} < T_{read}$, each current of an array pair generated by the same input challenge is characterized by a ratio greater than one equal to $G_I = I_{T_{read}}/I_{T_{ref}}$. The current comparison $I_1 - I_2$ at T_{ref} thus becomes the current comparison $G_{I_1} I_1 - G_{I_2} I_2$ at T_{read}. A bitflip event takes place when the two comparisons hold opposite results. Since each current is transformed into an associated voltage through the TIA stage, the bitflip event takes place when:

$$V_2 > \left| \frac{\Delta V}{G_{V_1} - G_{V_2}} \right| \cdot G_{V_1} \tag{7}$$

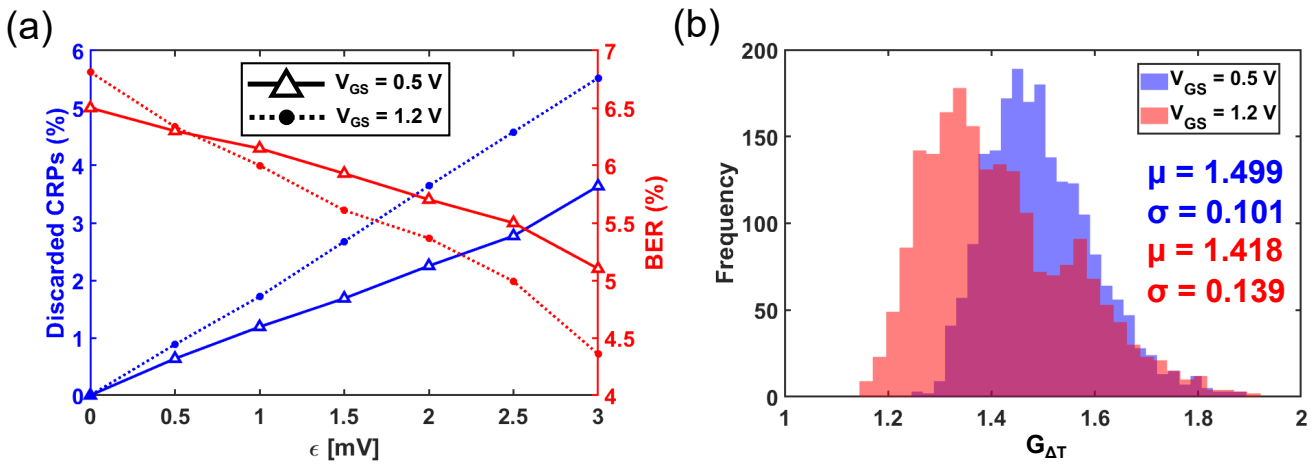


Fig. 7. (a) Bit error rate (BER) at 85℃ using a reference at 25℃ based on 128-bit keys, and percentage of discarded CRPs as a function of ε, with N = 5 and V_{READ} = 0.4 V. Using V_{GS} = 0.5 V improves the raw reliability of the solution at the cost of a lower percentage of CRPs recognized as unreliable due to the higher TIA gain (R_f = 60kΩ). Thus, the CRP selection scheme is less effective for lower V_{GS}. (b) Gain distribution of current operating points between 85℃ and 25℃ for V_{GS} = 0.5 V and V_{GS} = 1.2 V.

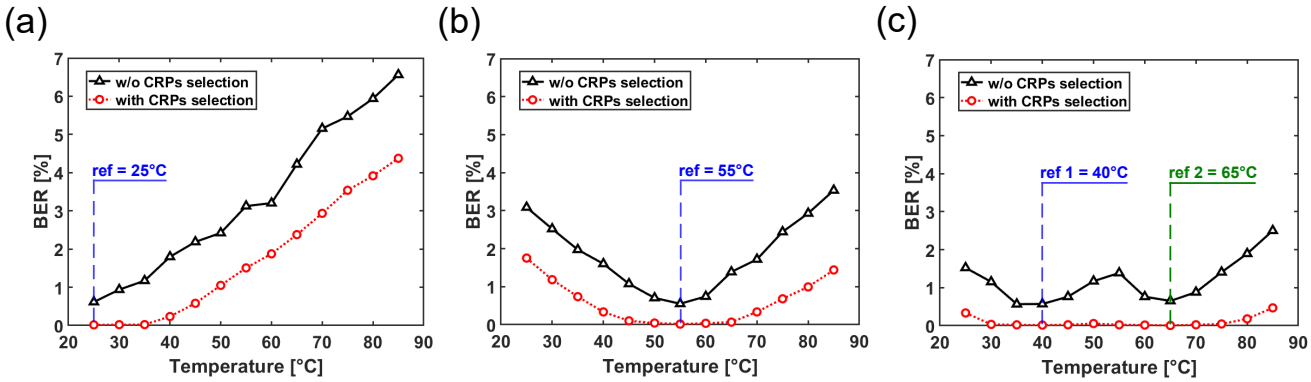


Fig. 8. Temperature reliability for V_{GS} = 1.2 V. (a) Average BER versus temperature for 128-bit keys, with a single enrollment @25℃ at 0.4 V. To enable CRP selection with a threshold of 3 mV, the percentage of discarded CRPs is 5.45%. (b) Average BER versus temperature for 128-bit keys, with a single enrollment @55℃ at 0.4 V. To enable CRP selection with a threshold of 3 mV, the percentage of discarded CRPs is 4.95%. (c) Average BER versus temperature for 128-bit keys, with double enrollment @40,65℃ at 0.4 V. In this scenario, the CRP selection scheme considers a CRP unreliable if during any of its enrollments it does not meet the threshold condition. To enable CRP selection with a threshold of 3 mV, the percentage of discarded CRPs is 7.73%.

where V_1, V_2 are the compared voltages at the output of the TIA stages at T_{ref}, $|\Delta V| = |V_1 - V_2|$, and G_{V_1}, G_{V_2} are the linear transformations of G_{I_1}, G_{I_2} in the voltage domain. The probability of satisfying Eq. (7) decreases at increasing mean value and at decreasing spread of the distribution of G.

A lower V_{GS} requires a higher TIA gain R_f, resulting in a lower number of CRPs identified as unreliable and thus discarded for the same ε, but also in a distribution of G with a higher mean value. This is possible due to the variation of the I-V curves of the PCM and MOSFET in weak inversion in the same direction with temperature. Fig. 7b shows the comparison between the distributions of the T-dependent current gain $G_I = I_{85°C}/I_{25°C}$ evaluated between T_{read} = 85°C and T_{ref} = 25°C, for the same 1T1R cells read at V_{READ} = 0.4 V using V_{GS} = 0.5 V and V_{GS} = 1.2 V, justifying the lower raw BER observed for V_{GS} = 0.5 V.

Fig. 8a shows a comparison between the raw BER and the BER obtained by applying the CRP selection scheme for the room temperature reference T_{ref} = 25°C and considering V_{READ} = 0.4 V, V_{GS} = 1.2 V, R_f = 20kΩ and ε = 3 mV. Discarding unreliable CRPs with this margin guarantees near-zero BER in the proximity of the reference temperature, and an overall benefit in terms of performance, with a percentage of discarded CRPs equal to 5.45% of the total. Fig. 8b shows the same analysis using as reference temperature T_{ref} = 55°C, discarding the 4.95% of the CRP space. Finally, Fig. 8c highlights the significant gain that can be achieved using two separate reference temperatures ($T_{ref,1}$ = 40°C, $T_{ref,2}$ = 65°C) and discarding each CRP that does not satisfy the condition $|\Delta V_{1,2}| > \varepsilon$ for any of the two temperatures during the respective enrollments. In this case, the amount of discarded CRPs is only slightly increased (7.73%).

The same considerations can be applied regarding variations of power supply with respect to the nominal case. For this study, different conditions of bias deviation around V_{READ} = 0.4 V were considered assuming two fixed gate-source voltages, namely V_{GS} = 0.5 V and V_{GS} = 1.2 V. Again, the bit-flip event can be described using Eq. 7, where G_V

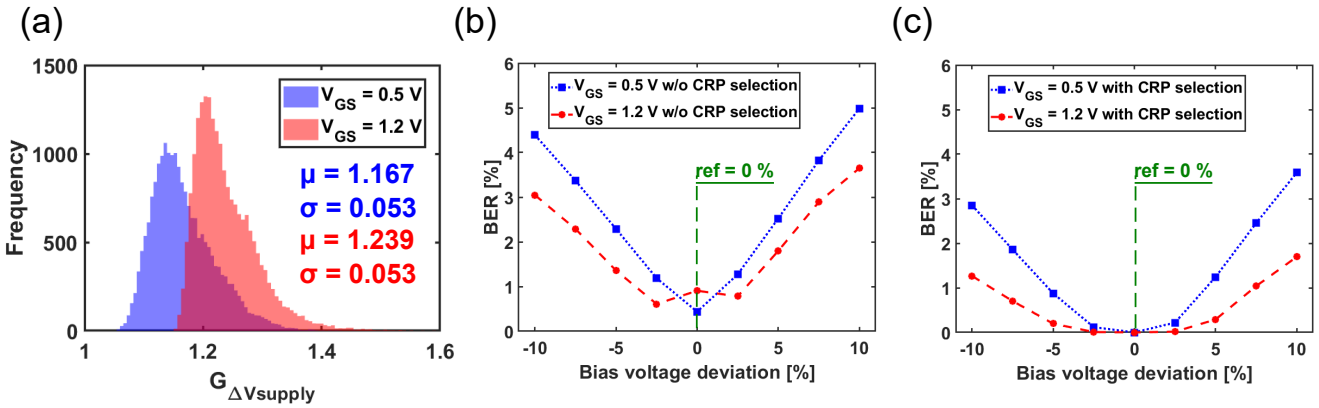


Fig. 9. Reliability against power supply variation. (a) Gain distribution of current operating points between +10% of bias voltage deviation and nominal condition, for V_{GS} = 0.5 V and V_{GS} = 1.2 V. (b) Average BER versus power supply deviation for 128-bit keys, with a single enrollment @0% at 0.4 V, for both V_{GS} = 0.5 V and V_{GS} = 1.2 V.(c) Average masked BER versus power supply deviation with CRP selection for 128-bit keys, with a single enrollment @0% at 0.4 V, for both V_{GS} = 0.5 V and V_{GS} = 1.2 V. To enable CRP selection with a threshold of 3 mV, the percentage of discarded CRPs is 3.58% for V_{GS} = 0.5 V (R_f = 60kΩ) and 5.45% for V_{GS} = 1.2 V (R_f = 20kΩ).

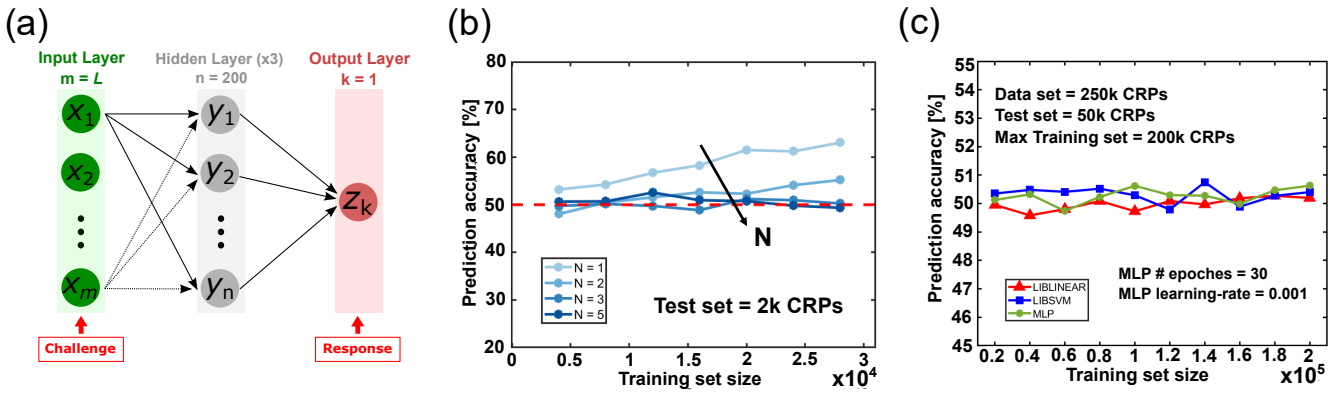


Fig. 10. ML-attack simulation. (a) Structure of the used MLP, for *L*-bit input challenges, 3 hidden layers with 200 nodes each and 1-bit response. (b) Modeling attack by MLP network, tested on 2k test set, as a function of training set size and number of selected cells (N). With only a few selected cells, the ease of mathematical modeling reflects the low entropy of the responses. (c) Average prediction accuracy for 40-bit challenges (*N* = 5), using three different machine learning models, as a function of training set size.

represents the voltage gain greater than one between the output of the TIA measured at $V_{READ} \pm \Delta V_{supply}$ and at V_{READ}. Fig. 9a shows the corresponding G_I distributions considering a voltage deviation of +10%, suggesting a worse BER versus voltage supply variations for small gate-source voltages. This behavior is due to the limited variation of the working point of the 1T1R cell when V_{READ} varies considering the MOSFET selector in weak inversion versus strong inversion. Furthermore, the increasing nonlinearity with the bias of the PCM I-V curve makes this variation more pronounced for positive ΔV_{supply}. Fig. 9b shows the BER as a function of the bias voltage deviation for the two gate-source voltage conditions without CRP selection, confirming the expected results. Fig. 9c shows the BER with CRP selection considering ε = 3 mV, requiring a percentage of discarded CRPs equal to 3.58% for V_{GS} = 0.5 V using R_f = 60kΩ. As in the previous case, the BER can be further mitigated by combining the CRP selection scheme with multiple enrollments at different V_{READ}, paying for a higher percentage of discarded CRPs.

D. Robustness to ML attacks

The security of strong PUFs is also measured in terms of resilience against mathematical clonability using modeling attacks, such as machine learning (ML) tools, when the adversary has access to a certain number of CRPs [4]. To evaluate machine-learning resilience, several ML techniques such as logistic regression (LR), support vector machines (SVM), and neural networks (NN) are widely applied in the literature due to their simplicity and effectiveness [21]. We used the online packages LIBLINEAR and LIBSVM to test the robustness of our PUF system against LR and SVM algorithms, respectively [20]. We also used a multi-layer perceptron (MLP) of size $40 \times 200 \times 200 \times 200 \times 1$ with rectified linear unit (ReLu) function as activation function for each layer as shown in Fig. 10a. For each algorithm, the size of the training set was increased from $2x10^4$ to $2x10^5$, using a subset of CRP exclusive to the test, equal to a quarter of the training set. Fig. 10b shows the prediction accuracy of the MLP as a function of the training set size and number *N* of selected WLs. The results show that selecting too few cells produces a more easily predictable response due to less entropy. Finally,

Fig. 10c shows the average prediction accuracy of the three machine-learning algorithms for $N = 5$ selected cells, which approaches the ideal 50% regardless of the size of the training dataset, supporting the robustness of the PUF system.

V. Conclusion

We presented a strong PUF based on embedded PCM cells in the virgin state, integrated in the 90 nm technology node. The pristine state shows promising properties for the implementation of PUF systems with enough entropy, moderate power consumption, and resilience against noise and environmental variations, thanks to the broad distribution of conductance and detailed CRP selection schemes. The PUF performance is fully supported by Monte Carlo simulations based on accurate modeling of the 1T1R PCM cell and array, integrated with parameters extracted from the design of the architecture implemented using a 90 nm commercial PDK. These results support PCM-based strong PUFs as a potential candidate for securing systems in IoT applications.

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] H. Nili *et al.*, "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.

[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] Q. Zhang, H. Chen, Y. Lu, X. Li, and Z. Song, "Design and security evaluation of PCM-based rPUF using cyclic refreshing strategy," *IEICE Electronics Express*, vol. 15, no. 10, pp. 20 180 239–20 180 239, 2018.

[6] N. Noor and H. Silva, "Phase change memory for physical unclonable functions," *Applications of Emerging Memory Technology: Beyond Storage*, pp. 59–91, 2020.

[7] F. Arnaud *et al.*, "Truly innovative 28nm FDSOI technology for automotive micro-controller applications embedding 16MB phase change memory," in *2018 IEEE International Electron Devices Meeting (IEDM)*. IEEE, 2018, pp. 18–4.

[8] D. Min *et al.*, "18nm FDSOI technology platform embedding PCM & innovative continuous-active construct enhancing performance for leading-edge MCU applications," in *2021 IEEE International Electron Devices Meeting (IEDM)*. IEEE, 2021, pp. 13–1.

[9] L. Cattaneo *et al.*, "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.

[10] 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.

[11] M. Baldo *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.

[12] E. Petroni *et al.*, "Advanced metrics for quantification of by-process segregation beyond ternary systems," *physica status solidi (RRL)–Rapid Research Letters*, vol. 17, no. 8, p. 2200458, 2023.

[13] S. Raoux, W. Wełnic, and D. Ielmini, "Phase change materials and their application to nonvolatile memories," *Chemical reviews*, vol. 110, no. 1, pp. 240–267, 2010.

[14] D. Ielmini and Y. Zhang, "Analytical model for subthreshold conduction and threshold switching in chalcogenide-based memory devices," *Journal of Applied Physics*, vol. 102, no. 5, 2007.

[15] D. Ielmini, "Threshold switching mechanism by high-field energy gain in the hopping transport of chalcogenide glasses," *Physical Review B*, vol. 78, no. 3, p. 035308, 2008.

[16] D. Ielmini and H.-S. P. Wong, "In-memory computing with resistive switching devices," *Nature electronics*, vol. 1, no. 6, pp. 333–343, 2018.

[17] R. Liu, P.-Y. Chen, X. Peng, and S. Yu, "X-point PUF: Exploiting sneak paths for a strong physical unclonable function design," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 65, no. 10, pp. 3459–3468, 2018.

[18] S.-H. Kwok, Y.-L. Ee, G. Chew, K. Zheng, K. Khoo, and C.-H. Tan, "A comparison of post-processing techniques for biased random number generators," in *IFIP International Workshop on Information Security Theory and Practices*. Springer, 2011, pp. 175–190.

[19] A. Rukhin *et al.*, *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. US Department of Commerce, Technology Administration, National Institute of ..., 2001, vol. 22.

[20] 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.

[21] P. Ren, Y. Xue, L. Jing, L. Zhang, R. Wang, and Z. Ji, "A strong physical unclonable function with machine learning immunity for Internet of Things application," *Science China Information Sciences*, vol. 67, no. 1, pp. 1–13, 2024.