CAS-PUF: Current-mode Array-Type Strong PUF for Secure Computing in Area Constrained SoCs

Dimosthenis Georgoulas, Yiorgos Tsiatouhas, Vasileios Tenentes
VCAS Lab, Dept. of Computer Science and Engineering
University of Ioannina
Ioannina, Greece
dgeorgoulas@cs.uoi.gr, tsiatouhas@uoi.gr, tenentes@uoi.gr

***Abstract*—Secure computing necessitates the integration in Systems-on-Chips (SoCs) of strong Physical Unclonable Functions (PUFs) that can generate a vast amount of Challenge Response Pairs (CRPs) for cryptographic keys generation, identification and authentication. However, the excessive area cost of strong PUF designs imposes integration difficulties to SoCs of area constrained applications, such as the IoT and mobile computing. In this paper, we present a novel strong PUF design, with silicon area requirements significantly lower than those of previous strong PUFs. The proposed Current-mode Array-type Strong PUF (CAS-PUF) is based on a current source topology of only six minimum size transistors, which is tolerant to power supply variation for enhanced reliability. Compared to previous strong PUFs, the CAS-PUF achieves the same number of CRPs with 20% to 72% less area size; while for the same area size, it provides 19 to 53 orders of magnitude higher number of CRPs. Furthermore, extensive Monte Carlo simulations on CAS-PUF show a reliability of 96.45% under ±10% power supply fluctuation; and 97.69% under temperature variation (0°C to 80°C), with an average uniqueness and uniformity of 50.01% and 49.54%, respectively. Therefore, CAS-PUF can be used as a hardware root of trust mechanism to secure computing in area constrained SoCs.**

***Index Terms*—Physical Unclonable Function - PUF, Current Mode, Strong PUF, CRP vs Area Efficiency, Secure Computing.**

I. Introduction

As technology evolves, new paradigms of hardware assisted secure computing are emerging for data encryption and hardware authentication. However, the storage of cryptographic keys and hardware IDs in memory, makes a system vulnerable to attacks that can leak the stored sensitive information. To address this vulnerability, Physical Unclonable Functions (PUFs) are gaining prominence. PUFs exploit the inherent imperfections in fabrication technology (variability) for static entropy harvesting and the generation of a unique, device-specific, binary response to be used as cryptographic key or hardware ID.

A PUF circuit is composed of several components defined by local parameter variations. Depending on the PUF approach these local parameters are combined, compared or directly read out to generate the binary output. Since the variation of the components cannot be controlled from the outside, a PUF cannot be replicated, making it unclonable. Depending on the application, the PUF output is determined by an input signal. Hence, a PUF is a function. To what extent the input signal influences the output differs between the various PUF approaches. The input (challenge) may alter the internal combination of the mismatching components, which changes the output (response). The input may also define which of the components should be used to generate the output [1].

PUFs map a set of challenges to a set of digital responses, forming challenge-response pairs (CRPs). Depending on how small or large the number of available CRPs is, a PUF is classified as weak or strong, respectively. A weak PUF can only support a small number of CRPs, and is vulnerable to tampering and brute force attacks. Strong PUFs are characterized by increased unclonability, since the complete determination/measurement of all CRPs within a limited time is not feasible [2]. Thus, they are ideal candidates for hardware authentication, which supports the hardware root of trust and thus secure computing. The strength of a PUF is generally determined by how the number of potential CRPs scales with the increasing PUF size. If the number of CRPs scales exponentially the PUF is considered strong, while linear or polynomial increment typically corresponds to weak PUFs [3].

Among various strong PUFs, we distinguish two main categories, digital PUFs like in [4], [5] and array-type PUFs. In the latter case, two main families exist, memory-based PUFs (like DRAM-based [6], [7], SRAM-based PUFs [8]–[12]) and custom array-type PUFs [13]–[16]. Memory-based PUFs have the advantage of reusing existing memory blocks in a chip; however, aiming to support the PUF operation, proper modifications in the memory topology are required. These modifications increase the design effort to meet the memory specifications and eventually affect speed performance and power consumption. Note that a) for the activation of the PUF mode of operation a latency is introduced to store the memory contents in a safe place, while before reentering the normal mode of operation it is required to restore back the memory contents, and b) during the PUF mode of operation the memory block is unavailable. Moreover, security issues arise since the memory blocks are accessible by other units in the chip. Finally, memory blocks are not always available in a design, or their modification to support PUF operation is not always feasible as they are intellectual property (IP) blocks. Custom array-type PUFs, are dedicated custom design PUF blocks, so they provide their response on demand without

978-3-9826741-0-0/DATE25/© 2025 EDAA

imposing any latency, they are in general simple, require less silicon area and may be more power efficient while they are more secure with respect to memory-based PUFs.

The Ring Oscillator PUF (RO-PUF) [4] is based on ring oscillators and counters for static entropy harvesting from the generated oscillation frequencies. The Arbiter PUF (APUF) [5] is based on paths' delay variations, exploiting cascaded switching elements to form multiple paths, plus an arbiter. The VTC-PUF [14] also uses cascaded blocks consisting of simple units with non-linear voltage transfer characteristic (VTC) and switches to construct delay paths. In Subthreshold Current Array PUF (SCA-PUF) [16], an array topology is used, which takes advantage of voltage differences generated by subthreshold current paths through properly biased, diode-connected, cascode PMOS transistors. An extension of the SCA-PAF is the TCO-PUF [13], which constructs voltage dividers by diode-connected, cascode PMOS and NMOS transistors in an array topology. The same concept is also exploited by the Proportional to Absolute Temperature (PTAT) PUF [15], which uses pairs of diode-connected transistors to form voltage dividers. Many works, including [8]–[12], have taken advantage of the intrinsic presence of SRAMs in modern integrated circuits to develop a PUF by reusing the memory circuitry. A simple SRAM-based PUF is presented in [8], which takes advantage of process variations in the cells during the start-up phase. In SPUF [12], the authors propose a modified 6T SRAM cell, with split wordlines, where whenever a group of four adjacent cells in the array is concurrently activated, process dependent bitflips may occur due to cell collisions. Also, the Strong in-Cache Bitflip PUF (SiCBit-PUF) [9] exploits an SRAM with in-memory computing capability to activate multiple cells in a column for bitflips generation. Since in both cases the use of arbiters or comparators is not required, high reliability levels can be achieved. The Array Current-Based SRAM (ACB-SRAM) PUF [10] monitors process dependent currents during the read operation of the memory. Compute In-Memory PUF (PUF-CIM) [11] uses a modified SRAM that supports in-memory computing, where the read currents of multiple activated cells in two bitlines are used for the response generation.

In this paper, we propose a current mode, custom array-type and strong PUF (CAS-PUF) that utilizes a low silicon area current source cell with reduced power supply variation dependency. In comparison to state-of-the-art custom array-type strong PUFs, the adopted topology offers a scalable PUF circuit design that provides higher numbers of CRPs (from 19 to 53 orders of magnitude) at significantly lower area requirements (from 20% to 72%), to support hardware root of trust for secure computing in area constrained SoCs. According to simulation results, CAS-PUF presents competitive characteristics with respect to uniqueness and uniformity metrics and high reliability levels over variations on temperature (0°C to 80°C) and power supply ($\pm 10\%$). Furthermore, CAS-PUF generates a latency-free response on demand, making it an ideal solution for applications with frequent use of security resources.

The organization of the paper is as follows. In Section II, the proposed current mode, array-type, strong PUF is presented. Section III analyzes the operation of the PUF, presents the PUF characterization results, and compares it with other strong array-type PUFs. Finally, Section IV draws conclusions.

II. Proposed Current Mode Array-Type PUF

The proposed CAS-PUF exploits a current source topology for the array cell, which is characterized by reduced dependency on power supply variations. A scalable array is constructed, where by increasing the number of rows, we enhance the number of Challenge-Response Pairs (CRPs), thereby strengthening the PUF's security features, while by increasing the number of columns the response size is increased.

A. CAS-PUF Cells

Fig. 1 depicts the proposed PUF cell, which is a modified version of a well-known current source that provides a current almost immune to power supply fluctuations [17]. It consists of three current mirrors formed by transistor pairs M1-M2, M3-M4 and M3-M5 respectively, plus a switch transistor M6. When M6 is ON, the current through the left branch (M1 and M4) is mirrored to the right branch (M2 and M3) by the current mirror M1-M2, while the current of the right branch is mirrored back to the left branch by the current mirror M3-M4. Thus, the circuit is self-biased and since each diode connected transistor is fed by a current source, the generated currents are relatively independent of Vdd.

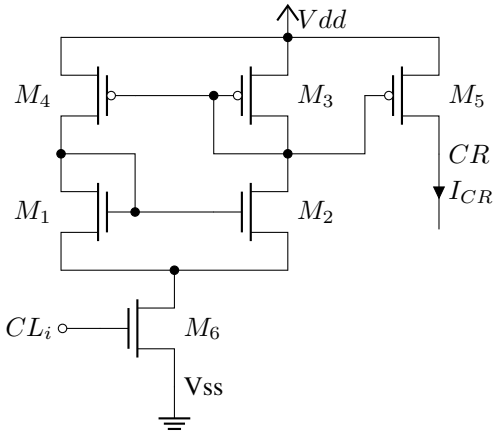

Fig. 1. Proposed 6T PUF cell.

The switch transistor M6 is added for the cell activation/deactivation. This device also mitigates the current leakage in the standby mode of operation. The gate of this transistor is driven by a bit (CL_i) of the challenge. Initially, when transistor M6 is OFF, no current flows through the cell and so the internal nodes, drains and gates of M3 and M4, are charging until all PMOS transistors reach the cut-off region. By turning M6 ON, a current begins to flow through each branch, which is defined by the transistor sizes and modulated by process variations. Finally, the current that is generated in the cell is delivered to the CR port through the third current mirror M3-M5. All six transistors in the cell should be of

minimum size and high threshold voltage transistors to keep silicon area and leakage current as low as possible, enhancing at the same time the effects of the process variations.

B. CAS-PUF Array Organization

The cells of the CAS-PUF are organized in an array structure (see Fig. 2), which aligns perfectly with the principles of a current-mode PUF. As a current-mode PUF, we define a PUF circuit where process variations dependent differences between the cells' currents determine the response.

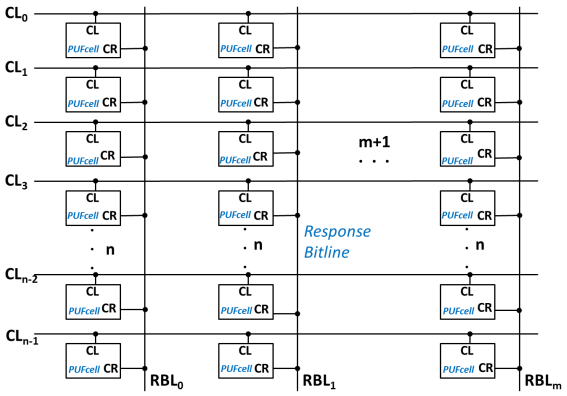

Fig. 2. The PUF array of n rows (CL) and $m+1$ columns (BL) of cells.

The PUF array consists of n rows and $m+1$ columns. The cells of a row are driven by the same bit of the challenge (CL_i), so that the challenge size is n bits. Thus, all cells in a row are concurrently activated or not. The cells of a column are connected to the same bitline (BL), through the CR port, feeding it with their currents when they are active. As multiple cells in a column can be simultaneously activated by a challenge to feed the common bitline (multiple rows activation), their currents are accumulated. Ideally, applying a challenge, the currents on all bitlines of the array are expected to be equal. However, due to process variations in the transistors of the cells, the generated currents differ, providing this way a static entropy harvesting mechanism for the proposed PUF. The currents of adjacent bitlines are compared with the use of a current comparator, so that $m+2$ current comparators are exploited, which generate an m bits response as shown in Fig. 3. Note that each bitline feeds two comparators, so that there are m effective comparators, plus two extra 'dummy' comparators to balance the load of the two bitlines at the left and the right side of the array.

C. The Current Mode Comparator and PUF operation

Since the PUF operates in current mode, which means that its response is provided by the comparison of current differences, a current mode comparator is required. For the validation of the proposed PUF operation as well as its performance characterization, we adopt the well-known Current Mode Sense Amplifier (see Fig. 4) as comparator [18]. Obviously, any current comparator in the literature can also be exploited instead. This circuit compares currents between

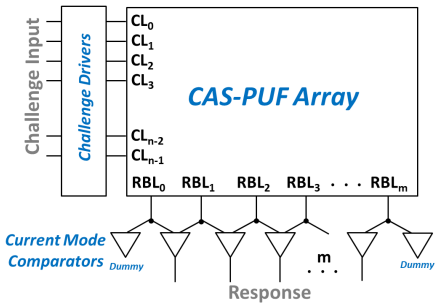

Fig. 3. The overall PUF architecture with the PUF array and the comparators.

two adjacent bitlines (BL). It is based on a CMOS cross-coupled latch (M1-M4). Transistors M5 and M6 are biased in the linear region and provide a low impedance clamp between the bitlines and ground. M7 and M8 are used as equalization devices, while M9 is a power switch. If $I_{BLL} > I_{BLR}$, then the response signal OUT is 0; otherwise, it is 1. Three control signals SA, EQ_1 and EQ_2 are exploited for circuit activation and fine tuning of its timing.

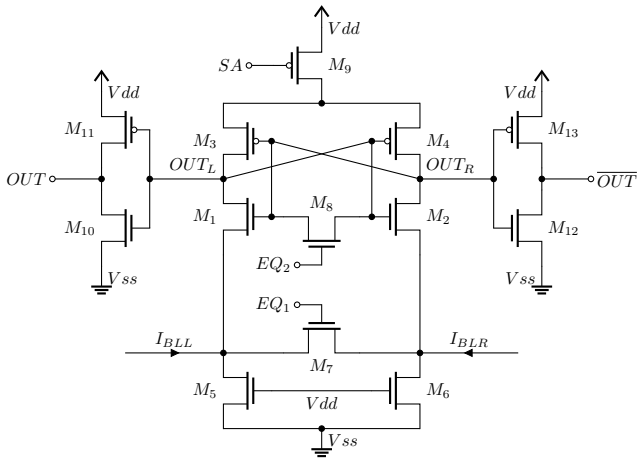

Fig. 4. The Current Mode Comparator.

The operation of the PUF circuit is divided into three distinct phases (discharge-equalization, activation, and sense) according to the comparator's functionality. Initially, in the discharge-equalization phase, the PUF remains inactive until a challenge is applied. Signals SA, EQ_1 and EQ_2 are set to high. Thus, the bitlines are discharged through the transistors M5 and M6 of the comparators in Fig. 4, while the internal nodes of the comparators are equalized to prevent biasing.

A challenge is then applied to the PUF, which enters the activation phase. Thus, one or more CL_i signal(s) turns to high and activate every PUF cell in the selected row(s) by setting ON the corresponding transistors M6. The current mirror M3-M5 of each activated cell supplies current to the relevant bitline. Once a stable current flows on the bitlines, the circuit transitions to the next phase.

In the final sense phase, the comparator is activated, setting the SA signal to low, to compare the currents of the

TABLE I
TRANSISTOR SIZES FOR THE PUF CELLS AND THE COMPARATOR.

	W/L (in nm)						
	M1-M2	M3-M4	M5-M6	M7-M8	M9	M10-M12	M11-M13
PUF Cell	120/80	120/80	120/80				
Comparator	1200/160	1200/160	1200/80	120/80	120/80	120/80	600/80

associated bitlines. At the beginning of this phase, the EQ_2 signal remains active to prevent leakage currents from causing imbalances in the cross-coupled inverters. Then, the EQ_2 signal is deactivated, allowing the comparator to generate the response. Afterwards, the circuit returns to the idle state (discharge-equalization phase). The phases and the signals' timing diagram are depicted in Fig. 5.

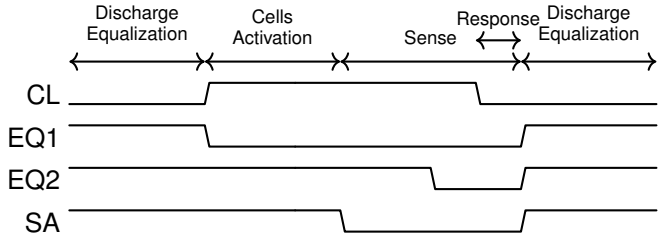

Fig. 5. PUF circuit timing diagram.

III. EVALUATION RESULTS

To evaluate the performance and robustness of the proposed PUF, we conducted extensive simulations on a relevant CAS-PUF array.

A. CAS-PUF Circuit Design

For the PUF design, we used the commercial CMOS technology of UMC at 90nm, exploiting the Virtuoso platform of Cadence. This design consists of an array of 256 rows by 65 columns of cells and 66 comparators, plus 256 drivers to apply the challenge. Initially, for the PUF cell we selected minimum size transistors to minimize the required silicon area. Note that in SRAM-based PUFs the cell always require more silicon area with respect to our cell, as not all transistors are of minimum size in order to be able to support the memory operation. For the comparator, our aim was to design a fast and low-power comparator with adequate resolution. Considering speed performance, we choose low threshold voltage transistors (LVT) on the cross-couple inverters and the output inverters to minimize the sense phase and get a fast response. Moreover, we selected to increase the size of the transistors in the cross-couple inverters in order to minimize the impact of process variations. The equalization transistors M7 and M8 are of minimum size. For the power switch transistor M9 we choose high threshold voltage transistors (HVT) to minimize the leakage current. The size of M5 and M6 transistors of the comparator significantly influences the PUF's performance, thus, according to [18], we selected sized transistors to keep them in the linear region of operation.

B. PUF Evaluation Metrics

To evaluate the performance of a PUF and compare it with other implementations, a set of key evaluation metrics must be employed [19]. Three widely used metrics are Uniqueness, Uniformity and Reliability. Initially, it is essential to define Hamming Distance and Hamming Weight since they play a crucial role in the expression of these metrics.

Hamming Distance: The Hamming distance $HD(a,b)$ between two words $a = (a_i)$ and $b = (b_i)$ of length n is defined to be the number of positions where they differ, that is, the number of (i)s such that $a_i \neq b_i$.

Hamming Weight: Let 0 denotes the zero vector: $00\ldots0$, The Hamming Weight HW(a) of a word $a = a_1$ is defined to be $d(a,0)$, the number of symbols $a_i \neq 0$ in a.

Uniqueness: Defines, using the 'Inter-chip Hamming Distance', the ability of one PUF instance to have a uniquely distinguishable behavior compared to the same PUF in a different chip. If two chips, i and j $(i \neq j)$, have n-bit responses, $R_i(n)$ and $R_j(n)$, respectively, for the challenge C, the average inter-chip HD among k chips is defined as:

$$HD_{\text{Inter}} = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(R_i(n), R_j(n))}{n} \times 100\% \tag{1}$$

Uniformity: Estimates how uniform the PUF's responses are and is defined as the proportion of 0's and 1's in the response bits. For a truly random response it is 50% and it can be calculated using the average Hamming Weight of k responses with r_i the Hamming Weight for each ith response, as follows:

$$Uniformity = \frac{1}{k} \sum_{i=1}^{k} r_i \times 100\% \tag{2}$$

Reliability: Measures, using the 'Intra-chip Hamming Distance', the ability of the PUF to generate an unaltered response R for a challenge C, under any changes in the conditions of the environment such as the ambient temperature and power supply. If a single chip (i), has the n-bit reference response $R_i(n)$ at normal operating conditions and the n-bit response $R'_i(n)$ at different conditions for the same challenge C, the average intra-chip HD for k samples/chip is defined as:

$$HD_{\text{Intra}} = \frac{1}{k} \sum_{j=1}^{k} \frac{HD(R_i(n), R'_i(n))}{n} \times 100\% \tag{3}$$

and so, the Reliability of the PUF can be defined as:

$$Reliability = 100\% - HD_{\text{Intra}}$$

C. CAS-PUF Circuit Characterization

For the evaluation of the CAS-PUF circuit, we executed five Monte Carlo analysis sessions, using the Spectre simulator and exploiting the statistical models of the technology used. Each session comprises 10,000 runs, to ensure an extended exploration of the PUF's behavior under process variations. In these simulations, we considered a range of temperatures

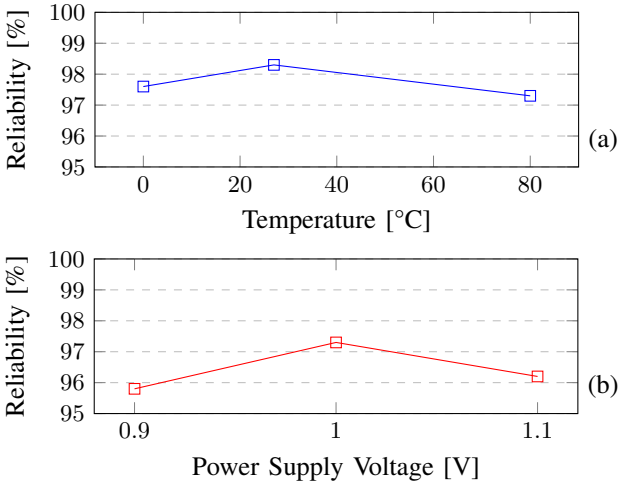

Fig. 6. Reliabilities during: (a) Temperature variations at constant power supply of 1V, (b) Power supply variations at constant temperature of 27°C

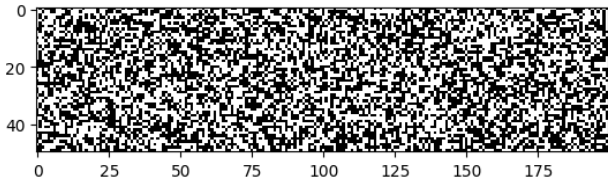

Fig. 7. Visual representation of Monte Carlo simulation results of PUF responses at 27°C and 1V. Black pixels correspond to binary value 0 and white pixels correspond to binary value 1.

from 0°C to 80°C, to account a variety of operating conditions. Furthermore, we perform corner case analysis of $\pm 10\%$ power supply fluctuations to the nominal voltage value of 1V (0.9V and 1.1V). As challenge to the PUF, we consider the case of 128 enabled rows. The reliability results for the PUF, according to the average values by the Monte-Carlo runs, are presented in both Fig. 6 (a) and (b) for temperature and voltage variations, respectively. In both cases, we observe a reliability greater than 95.8% with a variability less than 0.8%.

Overall, the reliability of the CAS-PUF ranges between 95.8% and 97.3% under power supply variations with an average value of 96.45% and a variability of 0.8%. This behavior was anticipated, as the PUF utilizes current generation cells with reduced power supply dependency. Moreover, it ranges between 97.28% and 98.25% under temperature variations with an average value of 97.69% and a variability of 0.5%. Additionally, the average measured uniformity and uniqueness of the PUF were 50.01% and 49.54%, respectively.

To measure the randomness of the PUF, we calculate the entropy of the PUF responses [19]. Ideally, this value should be 1, quantifying the unpredictability of a discrete random variable. Given that the PUF output consists of binary states ('0' and '1'), we use binary entropy:

$$H(p) = -p\log_2(p) - (1-p)\log_2(1-p) \tag{4}$$

where p is the probability of one of the two values. The measured entropy value is 0.99, indicating near-ideal randomness, as it is visualized in Fig. 7, which shows responses from 10,000 PUF instances using the same challenge.

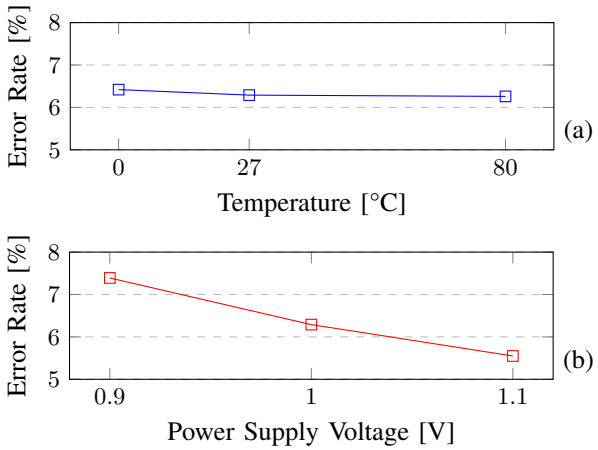

Fig. 8. Error rate of comparator decisions across: (a) Temperature variations, (b) Voltage variations.

Considering the adopted current comparator, we observed that on average makes incorrect decisions, with respect to the actual bitline current differences, at 6.37% of the time under varying temperature and power supply conditions. Among these incorrect decisions, 31.12% are unacceptable with respect to temperature variations and 41.06% are unacceptable with respect to power supply variations. An incorrect decision is unacceptable if for a PUF instance at least one response under specific temperature or power supply conditions differs from the rest responses of this instance under different temperature or power supply conditions. The rest incorrect decisions are acceptable since they do not invalidate the PUF operation. Fig. 8 illustrates that the number of incorrect decisions made by the comparator decreases as the supply voltage or temperature increases.

For the power consumption assessments of the proposed PUF, we consider a topology of 256 rows x 65 columns and a challenge that activates 128 rows. At 1V and 27°C, the resulting dynamic and static power consumption per response bit were measured at $3.23mW/b$ and $78.11nW/b$ respectively. Moreover, for an estimation of the required silicon area of this PUF, we take into account the area of the transistor gates ($W \times L$). The PUF array occupies an estimated silicon area equal to $958.464\mu m^2$, the row drivers occupy an area equal to $56.53\mu m^2$, while the current comparators require an estimated silicon area equal to $72.9\mu m^2$. Therefore, the estimated total silicon area occupied by the PUF is $1087.9\mu m^2$.

D. Challenge-Response Pairs

According to the CAS-PUF operation, it is feasible to simultaneously activate multiple rows using any combinations of the n available rows. Choosing to activate k rows, the

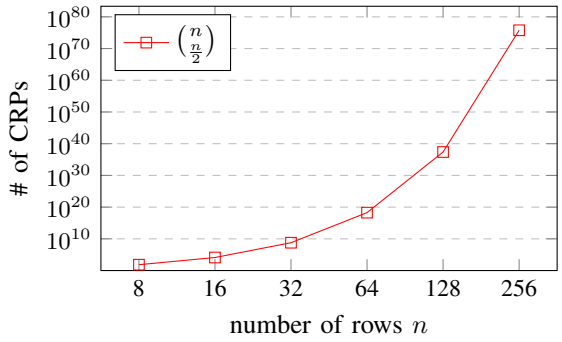

Fig. 9. Exponential increase in CRPs as the number of PUF array rows increases when selecting $\frac{n}{2}$ activated rows.

number of CRPs is expressed by the next equation:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{5}$$

which provides the number of combinations of n available rows per k activated rows. The maximum number of CRPs is achieved by choosing a challenge that activates half of the available rows ($\frac{n}{2}$). Fig. 9 depicts the exponential increment of the CRPs by scaling up the PUF array. Thus, the CAS-PUF is a strong PUF. For example, in an array with 256 rows, choosing to activate a number of 128 rows ($n = 256$ and $k = 128$) we get roughly 5.76×10^{75} CRPs.

E. Comparisons

Next, we compare the reliability, uniqueness, and uniformity of the proposed CAS-PUF against state-of-the-art custom array-type and strong PUFs; whose data, gathered from the literature, are shown in Table II. In addition, in Fig. 10, we compare their number of CRPs, with respect to their silicon area cost. The area cost is evaluated by the number of minimum size transistors (MST) in each array. The CAS-PUF provides the same number of CRPs with 20% to 72% fewer MSTs; while for the same number of MSTs, it provides a 19 to 53 orders of magnitude higher number of CRPs.

IV. Conclusions

In this paper, we present a new current mode, custom array-type and strong Physical Unclonable Function (PUF) circuit.

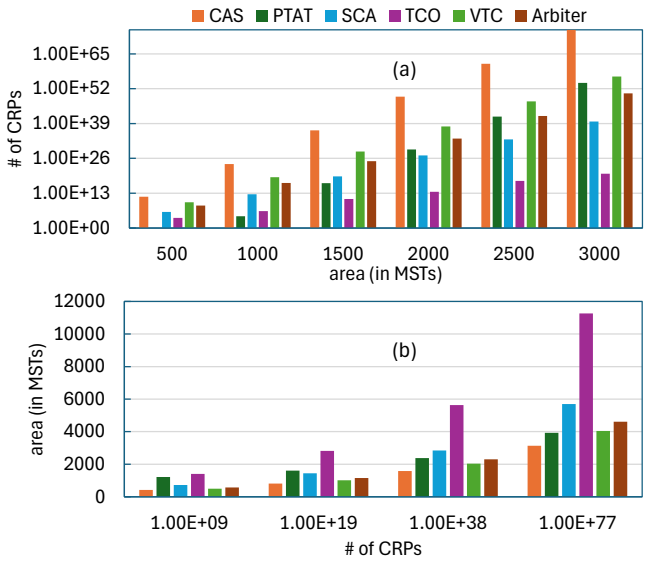

Fig. 10. Comparisons among array-type strong PUFs in terms of a) number of CRPs for the same area and b) area for the same number of CRPs.

It is characterized by enhanced reliability over temperature and power supply variations, and significantly lower silicon area requirements with respect to earlier custom array-type and strong PUF designs. The comparisons shown that the proposed PUF achieves the same number of CRPs with more than 20% less area or for the same area, it provides more than 19 orders of magnitude higher number of CRPs. According to simulation results on the design of the PUF in a $90nm$ technology, the estimated reliability under temperature variations is 97.69%, while under voltage variations is 96.45%. Since the proposed PUF is based on a power supply independent cell topology, its reliability is less sensitive on voltage variations. The uniformity and the uniqueness of the PUF have been measured to be 49.54% and 50.01% respectively.

References

[1] C. Böhm and M. Hofer, *Physical unclonable functions in theory and practice*. Springer Science & Business Media, 2012.

[2] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

TABLE II
COMPARISON BETWEEN STATE-OF-THE-ART CUSTOM ARRAY-TYPE STRONG PUFS AND THE PROPOSED CAS-PUF

Design	**Arbiter PUF [5]**	**PTAT-PAF [15]**	**SCA-PUF [16]**	**TCO-PUF [13]**	**VTC-PUF [14]**	**Proposed CAS-PUF**
Technology	45nm	65nm	130nm	130nm	45nm	90nm
Variability Parameter	Delay	Current	Current	Current	Delay	Current
Temperature Range (^{o}C)	0 – 100	0 – 80	-20 – 80	-40 – 125	0 – 85	0 – 80
Voltage Range (V)	0.9 – 1.1	0.6 – 1.2	1.08 – 1.32	0.97 – 1.32	0.9 – 1.1	0.9 – 1.1
Reliability (T=c) %	97.01	99	NA	NA	96.20	96.45
Reliability (V=c) %	94.49	96.5	NA	NA	96.25	97.69
Avg. Reliability	NA	NA	91,00	91.58	NA	NA
Uniqueness %	49.99	50.01	49.9	50.23	NA	50.01
Uniformity %	50.09	49.3	52.08	NA	50.1	49.54

[3] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "A PUF taxonomy," *Applied Physics Reviews*, vol. 6, no. 1, 2019.

[4] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *44th Design Automation Conference (DAC)*, 2007, pp. 9–14.

[5] M. Moradi, R. F. Mirzaee, and S. Tao, "CMOS arbiter physical unclonable function with selecting modules," in *20th International Symposium on Computer Architecture and Digital Systems (CADS)*. IEEE, 2020, pp. 1–6.

[6] A. Schaller, W. Xiong, and et al, "Intrinsic Rowhammer PUFs: Leveraging the Rowhammer Effect for Improved Security," in *Int. Symp. on Hardware Oriented Security and Trust (HOST)*. IEEE, 2017, pp. 1–7.

[7] E. Abulibdeh, L. Younes, B. Mohammad, K. Humood, H. Saleh, and M. Al-Qutayri, "DRAM-Based PUF Utilizing the Variation of Adjacent Cells," *IEEE Transactions on Information Forensics and Security*, vol. 19, no. 1, pp. 2909–2918, 2024.

[8] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *9th International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*. Springer, 2007, pp. 63–80.

[9] A. Xynos, V. Tenentes, and Y. Tsiatouhas, "SiCBit-PUF: Strong in-Cache Bitflip PUF Computation for Trusted SoCs," in *IEEE European Test Symposium (ETS)*. IEEE, 2023, pp. 1–6.

[10] F. Zhang, S. Yang, J. Plusquellic, and S. Bhunia, "Current based PUF exploiting random variations in SRAM cells," in *Design, Automation & Test in Europe Conference (DATE)*. IEEE, 2016, pp. 277–280.

[11] Z. Chen, M. Wu, Y. Zhou, R. Li, J. Tan, and D. Ding, "PUF-CIM: SRAM-based compute-in-memory with zero bit-error-rate physical unclonable function for lightweight secure edge computing," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 31, no. 8, pp. 1234–1247, 2023.

[12] L. Lu, T. Yoo, and T. T.-H. Kim, "A 6T SRAM based two-dimensional configurable challenge-response PUF for portable devices," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 69, no. 6, pp. 2542–2552, 2022.

[13] M. S. Mispan, B. Halak, Z. Chen, and M. Zwolinski, "TCO-PUF: A Subthreshold Physical Unclonable Function," in *11th Conf. on Ph.D. Research in Microelectronics & Electronics (PRIME)*. IEEE, 2015, pp. 105–108.

[14] A. Vijayakumar and S. Kundu, "A Novel Modeling Attack Resistant PUF Design based on Non-linear Voltage Transfer Characteristics," in *Design, Automation & Test in Europe Conference (DATE)*. IEEE, 2015, pp. 653–658.

[15] J. Li and M. Seok, "Ultra-compact and robust physically unclonable function based on voltage-compensated proportional-to-absolute-temperature voltage generators," *IEEE Journal of Solid-State Circuits*, vol. 51, no. 9, pp. 2192–2202, 2016.

[16] H. Zhuang, X. Xi, N. Sun, and M. Orshansky, "A strong subthreshold current array PUF resilient to machine learning attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 67, no. 1, pp. 135–144, 2019.

[17] B. Razavi, *Design of analog CMOS integrated circuits*. McGraw-Hill, 2005.

[18] T. N. Blalock and R. C. Jaeger, "A high-speed clamped bit-line current-mode sense amplifier," *IEEE Journal of Solid-State Circuits*, vol. 26, no. 4, pp. 542–548, 1991.

[19] B. Halak, *Physically unclonable functions*. Springer, 2018.