Journal of Electronic Testing (2023) 39:611–620
https://doi.org/10.1007/s10836-023-06085-4

A Low Bit Instability CMOS PUF Based on Current Mirrors and WTA Cells

Joseph Herbert Mitchell-Moreno[1] · Guillermo Espinosa Flores-Verdad[1]

Received: 20 June 2023 / Accepted: 7 September 2023 / Published online: 15 September 2023

Abstract

In this work the electrical behaviour of CMOS winner take all (WTA) cells is exploited to create a novel topology for physical unclonable functions (PUF) using current mirrors. The basic cell is based on low cascode current mirrors and high-gain Sekkerkiran WTA cells. These cells are capable to select a winner neuron according to manufacture process variations. Post-layout validation of the cell was performed using Cadence Virtuoso tools with a 65nm UMC technology. The PUF energy consumption is 5.670pJ/b with native bit instability of 2.294% among 1024 readings considering temperature variations. The PUF performance is quantified with uniqueness, uniformity and reliability metrics yielding results of 49.614%, 49.662% and 97.706% respectively among 1000 considered instances. An average inter-HD=49.837%, and intra-HD=1.570% are obtained assuming temperature variation from (-20C ~ 120C) and 300mV of supply voltage fluctuation, the key generation latency is 73ns (8b), while the true randomness of keys is proved by NIST and autocorrelation function (ACF) tests.

Keywords Physical unclonable functions · Hardware security · CMOS design · Winner take all · Key generation · Authentication

1 Introduction

With the rapid advancement of technology, silicon integrated circuits (ICs) have become essential components in electronic devices, ranging from smartphones to critical industrial control systems. This increased reliance on such devices has also raised significant concerns regarding the security of their hardware. Hardware security issues encompass vulnerabilities that can be exploited to manipulate, gain unauthorized access, or compromise the secure functioning of integrated circuits. These vulnerabilities can be utilized to acquire sensitive information, such as cryptographic keys, intellectual property (IP), or even to execute malicious attacks with the purpose of stealing sensitive information [14]. Previously, several alternatives were used to store sensitive data in ICs; however, these alternatives presented significant drawbacks compromising at least one along of the integrity, reliability, or availability of the information [7]. Non-volatile memories can store sensitive information, but their vulnerability to physical attacks or tampering by third parties makes them a high-risk option [18], on the other hand, using tokens as storage devices is a costly and complex alternative that increases the overall complexity and costs of the system.

In CMOS technology, unavoidable phenomena due to the constant reduction in FET channel lengths over the years, such as variation process and mismatch can be exploited in analog systems for security-focused purposes by means of the physical device [20]. Physical unclonable functions (PUFs) were introduced in the early 2000s as a promising concept to implement a solution for hardware security purposes [5]. Since PUFs in silicon extract the unique physics characteristics produced during the manufacturing process of an IC, which are exploited to obtain challenge-response pairs (CRPs) that works as a hard to clonate identifier at a very low production and energy cost [2]. From then on several works have been proposed focused on leveraging PUFs in a wide range of applications, such as device authentication, key generation, random number generation, IP protection, anti-counterfeiting of data bases cloning for electronic transactions among others , [1, 22]. Unfortunately,

Responsible Editor: N. Karimi

Joseph Herbert Mitchell-Moreno and Guillermo Espinosa Flores-Verdad contributed equally to this work.

✉ Joseph Herbert Mitchell-Moreno
joseph.mitchell1906@gmail.com

Guillermo Espinosa Flores-Verdad
gespino@inaoep.mx

[1] Electronics Department, Instituto Nacional de Astrofísica, Óptica y Electrónica, Luis Enrique Erro 1, San Andres Cholula 72840, Puebla, Mexico

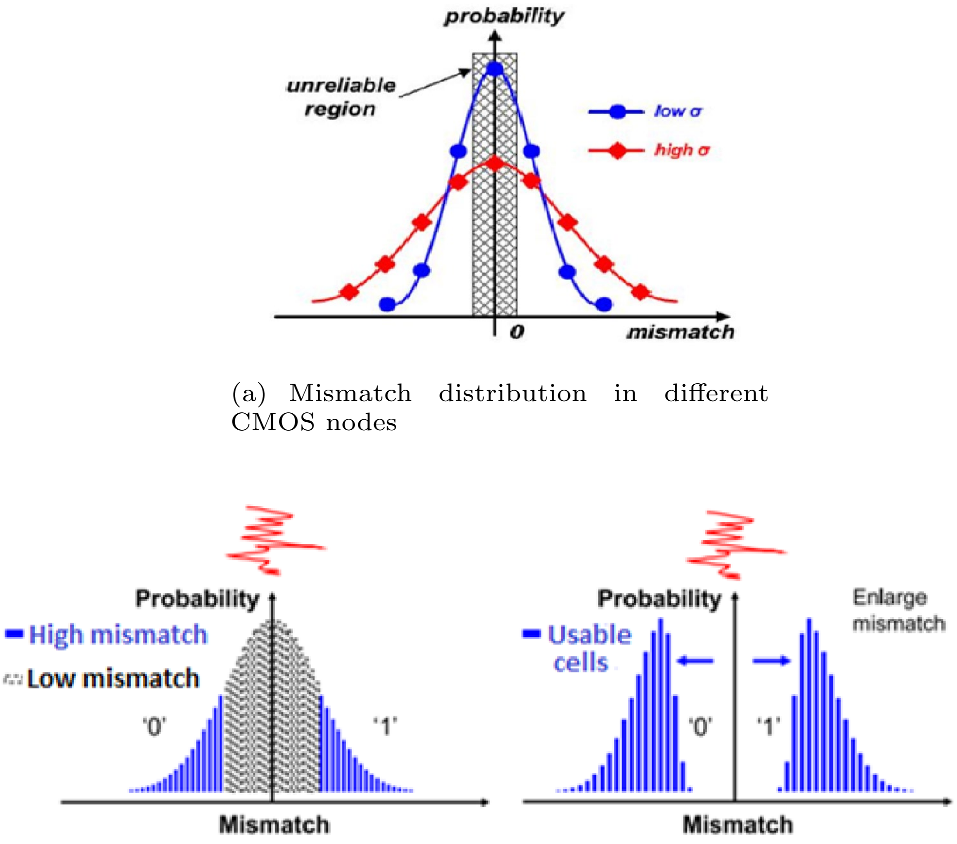
environmental variations such as temperature and voltage affect PUFs increasing erroneous responses, which leads to the generation of false keys [10]. The raw key can be synthesized by error correcting codes or helper data algorithms in order to be validated [19]. However, the use of post-processing stages open access doors for attackers and increase the system overall consumption energy.

For this proposal, the high gain of the cell along with output logic circuitry, reduces the zone of low reliability to almost 0, allowing any mismatch to be used to create reliable responses. Fig. 1(a) shows two curves representing two chips in different CMOS technologies and their mismatch dispersion. This contrast reveals that older technologies (longer channel) would present less dispersion and therefore a higher probability of falling into unreliable zones compared to smaller-sized technologies. Fig. 1(b) demonstrates how an different approach transforms the PUF keys from a normal distribution into a profile where the majority of bits are secure.

In this work a PUF topology with energy consumption of 5.67pJ/b based on CMOS current mirrors and winner take all (WTA) cells is proposed. In order to generate random keys from a macro, the WTA cells are used as current comparators [4]. Without using any additional post-processing stage, the raw keys obtained were validated as safe due to an Intra-PUF variation of 1.570% when temperature variations from (-20C ~ 120C) and ±10% of the nominal voltage are considered. The proposed PUF achieves uniqueness and uniformity metrics of 49.614% and 49.662% respectively, with a native bit instability of 2.294%. In addition the true variability of the PUF is demonstrated with the standards of the National Institute of Standards and Technology (NIST) [21] and the autocorrelation function (ACF) [15].

2 Winner Take All Cells

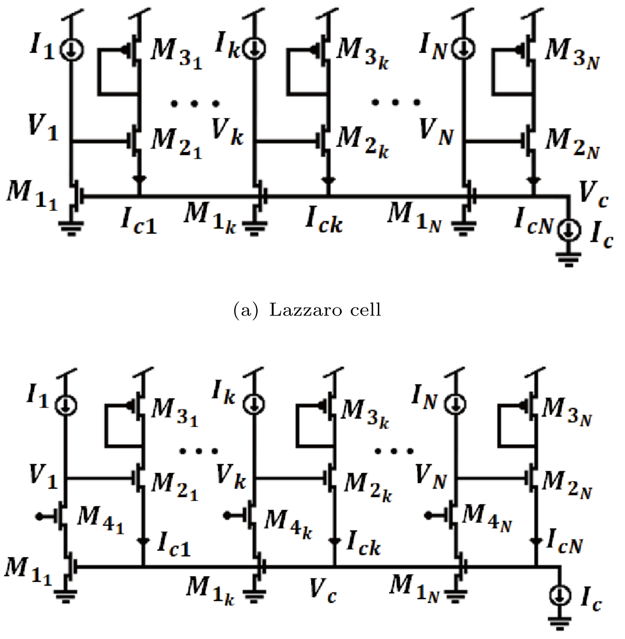
WTA cells are structures widely used in neural network hardware implementations capable of selecting only one input and annulling the rest of them [6]. Lazzaro's cell was first proposed in [11], the circuit in Fig. 2(a) force N neurons to compete, allowing the winner to take all the current Ic, its operation is based on the inhibitory action that results from an imbalance in the cell. Let be the input currents I_1, I_k and I_N equal in magnitude, the sizing of mirrored transistor equal, while (↑) or (↓) indicate an increase and decrease of magnitude respectively, the inhibitory action exists when an imbalance in the input current such that $I_1 = I_k = I_N + \Delta I$ occurs, yielding $I_N \uparrow V_N \uparrow V_{gsM_{2N}} \uparrow I_{cN} \uparrow$, now, as all the



(a) Mismatch distribution in different CMOS nodes

(b) Mismatch distribution required for PUFs

Fig. 1 Effect of mismatch on output bits reliability. **a** Distribution of mismatch in reliability for systems in different technologies [9]. Greater dispersion occurs when smaller technologies are used, reducing the likelihood of having samples in the unreliable zone. **b** Usable cells must move away from the unreliable zone, which is visualized as "enlarging the mismatch"



(a) Lazzaro cell

(b) Sekkerkiran cell

Fig. 2 Schematic topology of multineuron two WTA cells

currents I_{c1}, I_{ck} and I_{cN} are tied to the same supply current I_c the other two starts to decrease their magnitudes, so that $I_{c1}\downarrow I_{ck}\downarrow$. Since I_1 and I_k can not increase, voltages $V_{dsM_{2_1}}\downarrow V_{dsM_{2_k}}\downarrow$ until $V_{ds}=V_{gs}-V_{th}$ and transistors reach triode region where $I_d=\mu C_{ox}\frac{W}{L}\left(\left(V_{gs}-V_{th}\right)V_{ds}-\frac{1}{2}V_{ds}^2\right)$, from this point onward, as long as the voltage V_{ds} continues to decrease, the current will also decrease until it is completely inhibited.

Based on the fact that Lazzaro's cell current gain (A_i) and R_{in} are small (Eqs. 1 and 2), Sekkerkiran proposed in [17] an improvement using cascodes at nodes $V_{1,k,N}$ to increase R_{in} and so A_i increases by the same factor (Eqs. 3 and 4), see Fig. 2(b). This increase in A_i benefits the inhibitory action by making it more sensitive to the input currents difference, requiring a lower ΔI to establish a winner neuron.

Basic design equations for Lazzaro WTA cell:

$$A_i = g_{m2_1} r_{o1_1} \tag{1}$$

$$R_{in} = r_{o1_1} \tag{2}$$

Basic design equations for Sekkerkiran WTA cell:

$$A_i = g_{m4_1} r_{o4_1} g_{m2_1} r_{o1_1} \tag{3}$$

$$R_{in} = g_{m4_1} r_{o4_1} r_{o1_1} \tag{4}$$

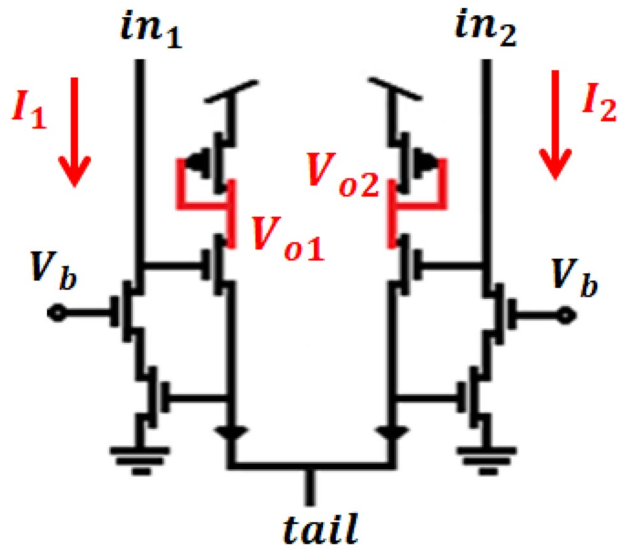


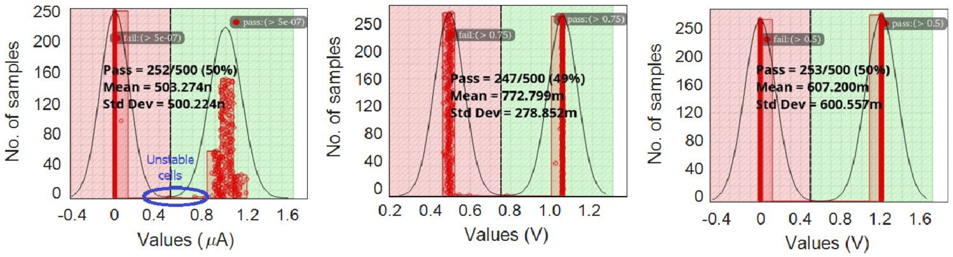
Fig. 3 Input currents as entropy sources using WTA circuits. Output nodes are also highlighted, these are not rail to rail

3 Proposed Basic Cell and PUF Macro

The basic unitary WTA cell utilized is deployed in Fig. 3. Input currents I_1 and I_2 are designed to be equal, but mismatch and process variations in current mirrors can force only one neuron to win, allowing to create two output states in nodes V_{o1} and V_{o2}. The foundations of the proposed PUF are based on this fact.

To work properly as a PUF, this cell has low-voltage cascode mirrors tied to input nodes in_1, in_2 and tail currents in *tail* (mirrors are not shown). It is important to carefully layout the input mirrors to minimize mismatch between them and avoid biasing the winner cell. The proposed topology takes advantage of mismatch to create the PUF response. In outcoming sections it will be demonstrated that the cell exhibits significant process variability with low sensitivity to temperature and voltage, making it suitable for use as a PUF. The dispersion of the winner current when Monte Carlo simulations are considered (only mismatch) is shown in Fig. 4(a). These currents lead to a raw response (V_{o1} or V_{o2}) that still needs to be improved since it is not rail-to-rail, as seen in Fig. 4(b). In Fig. 4(c), it is seen that by adding high gain AND and OR gates, it is possible to convert the outputs V_{o1}, V_{o2} to a single rail-to-rail voltage selected by the challenge V_{chall}. Fig. 5, allows to see that the AND gate receive the WTA's output and the challenge; the OR gate is able to set the PUF bit in V_o. Joining together several basic cells in Fig. 6, a PUF macro can be created, containing the response of the entire PUF. The footprint represents its digital identity, black and white squares are logic 0 and 1 states respectively.

Fig. 4 Scattering of logic states through the basic cell of the PUF



(a) WTA output currents

(b) WTA output voltages (raw keys)

(c) Output PUF bit (rail-to-rail)

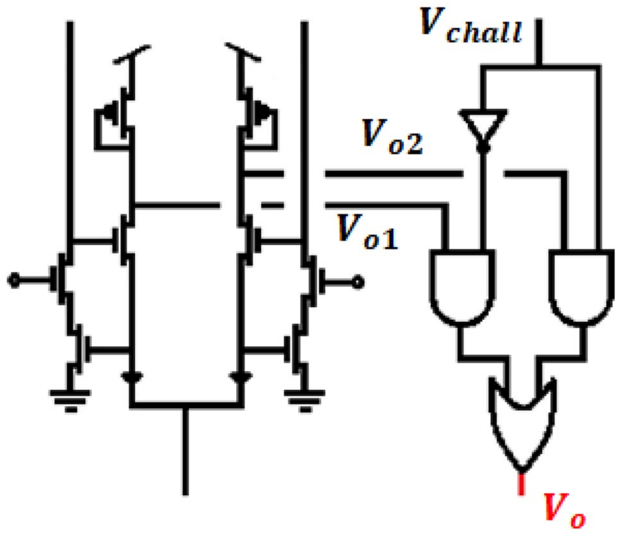
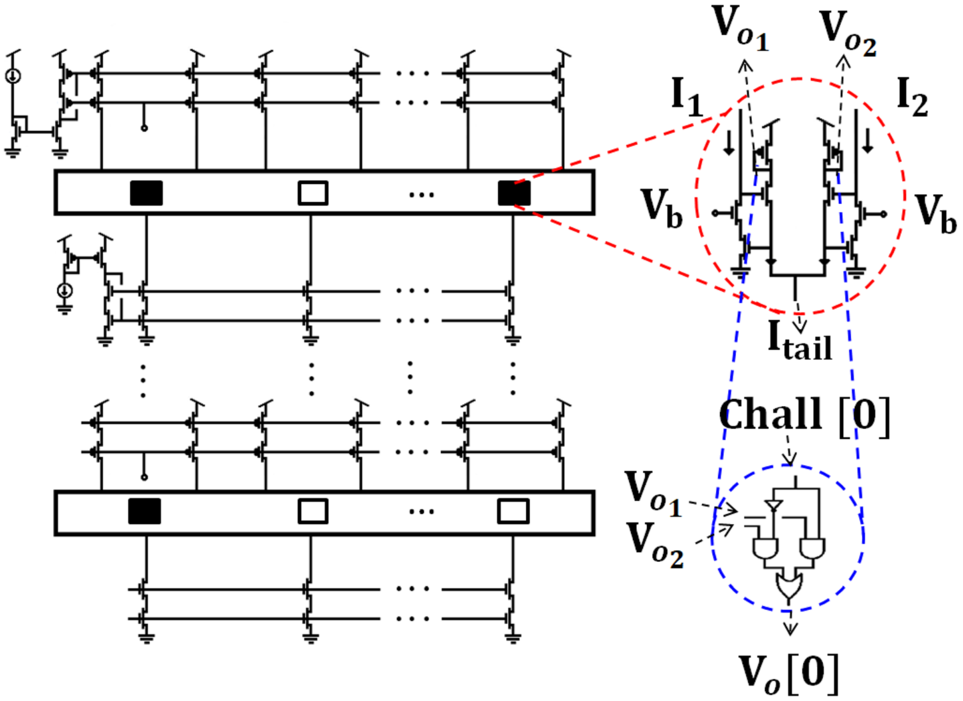


Fig. 5 PUF basic cell, with output node highlighted

By having a WTA cell with high gain and sensitive to process variations, it becomes possible to generate random outputs only dependent on IC's manufacture, if the input currents are implemented with low voltage cascode mirrors, parameters such as W, L, Vth will affect the replicas of I_{ref} leading to a winner neuron. Proposed PUF macro is shown in Figs. 6 and 7, where the entropy is mainly due to the amplitudes of the currents $I_{1,2}$ and mismatch along transistors of Sekkerkiran's core cell. In order to obtain a voltage signal at the output biased on gnd or V_{DD}, voltage buffers with CMOS inverters at the output nodes of each neuron are used to obtain the voltage $V_{out1,2}$ as strong states.

Performing DC analysis, obtaining the curve I_{out1} vs I_1, see Fig. 8(a), where the slope of the curves represents A_i and the sensitivity of the cell with respect to I_1 is represented by the region with slope different than 0. The immunity of the inhibitory phenomenon is validated by the similarity between the 6 curves (temperature and voltage are varied

Fig. 6 Schematic diagram of proposed macro, including low voltage current mirrors, WTA and output buffers



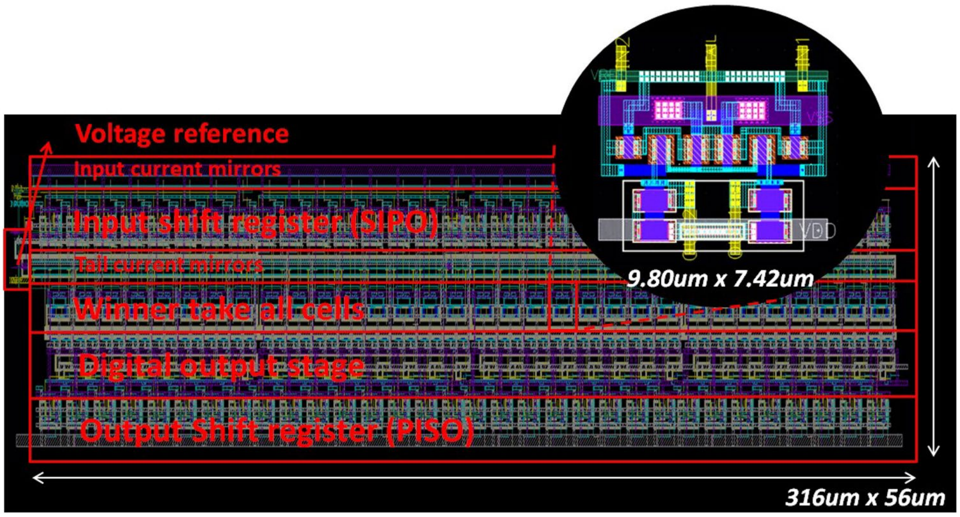


Fig. 7 Layout of the PUF including low voltage current mirrors and output buffers

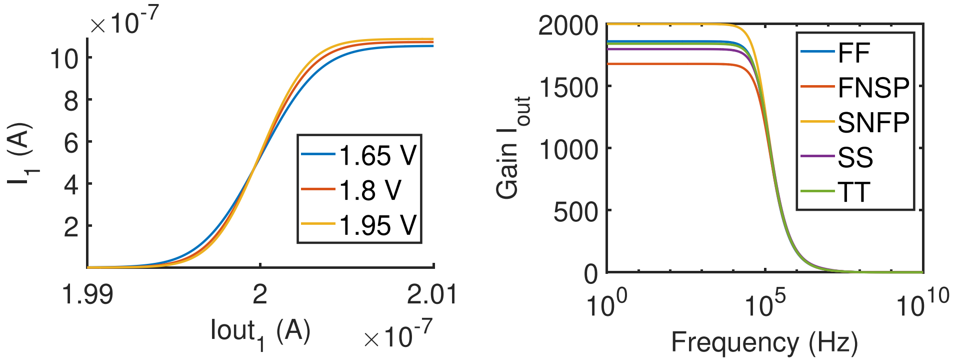
one at a time), and the sensitivity to mismatch is evidenced by the small ΔI required to carry the current I_1 from minimum to maximum value. Due to the implementation of (I_1 and I_2) with current mirrors, the gain of the PUF is strongly dependent on mismatch and process variation, as evidenced in Fig. 8(b) (process variation only, no mismatch). By grouping several PUF cells in an array, a macro PUF is created, Fig. 9, calling $n1$ the neuron on the left side and $n2$ on the right, these squares represent the polarization of each cell of the array, strong stages are included in black and white squares (white when $n1$ wins or black when it loses), the gray gamma (red circle) is used to represent the cells that do not achieve total inhibition (weak states), finally there are states that despite not achieving total inhibition (blue circle) are strong enough to set a safe bit. Transitory behaviour of cells is deployed in Fig. 10. In a PUF macro of NxM cells, certain properties must be fulfilled to guarantee randomness and reliability when used as PUF; The macro must be invariant, unpredictable and unbiased, while the cells must generate strong logical states, unpredictable, robust to environmental variations and sensitive to the process.

4 Results

In order to consider the IC's fabrication process variations and mismatch, monte carlo simulations on the PUF macro are run with Cadence Virtuoso©. To valide PUF's entropy true randomness in this technology, NIST and ACF tests are performed at nominal conditions, in addition, the reliability and uniqueness are characterized considering different environmental operating conditions in the following subsections.

4.1 Inter-PUF and Intra-PUF Measurements

As seen in Fig. 11(a), the ability to differentiate different PUF over others and its robustness against V_{DD} and temperature variations are demonstrated by inter and intra-HD respectively, 1000 chips of 100 bits each are simulated obtaining a gaussian form for inter-HD with μ = 49.837%, σ = 4.984%. For intra-HD, 100 measurements were made with V_{DD} variation of ±0.12V over the nominal value of



(a) Inhibition characteristic for different VDD

(b) WTA's current gain for different corner process

Fig. 8 DC and AC characteristics including variations for voltage, temperature (not displayed), and process

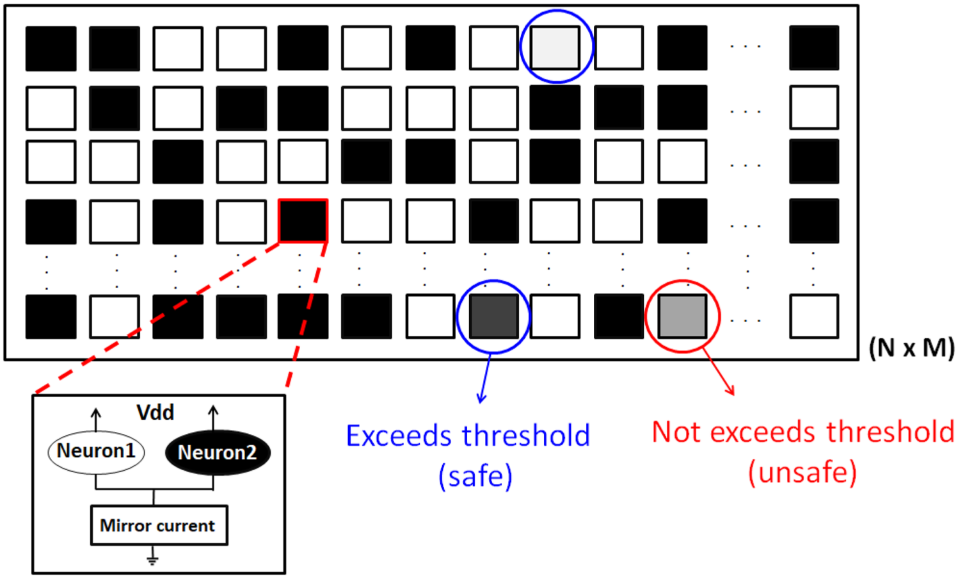


Fig. 9 PUF macro, grayscale colors squares represent the steadiness of the output bits

1.2V, and temperature from (-20C ~ 120C), obtaining values of $\mu = 1.570\%$ and $\sigma = 0.766\%$, it also exhibits separations of 32X among intra and inter-PUF distributions. As it was previously shown in Fig. 4, the response from a single 500-bit instance is used to determine the percentage of unstable outputs bits. An unstable bit is produced by the PUF when mismatch and process variation together are unable to establish a winner neuron for any temperature. The dots out of the bars on the extremes, represent more sensitive cells, being 2.2% of the total bits (11 out of 500). Measurements of the same PUF instance under the same challenge were performed to verify the behavior of unstable bits in Fig. 11(b), where the (32 x 32) bit array footprint is displayed. It is observed that among temperatures of -20C, 60C and 120C, there were 18 non-reliable cells, yielding a bit flipping rate of 1.758%. (For a test performed in the array of (64 x 64) the bit flipping rate obtained was 2.142%).

4.2 Uniqueness, Uniformity and Bit-Aliasing

Uniqueness is a measure that allows a PUF instance to be individualized from a group of PUFs of the same type. If k devices are considered, the uniqueness between the PUF instances PUF_i and P_j which produce R_i and R_j responses is calculated as:

$$(Uniq) = \frac{2}{k(k-1)} \sum_{i=1}^{(k-1)} \sum_{j=i+1}^{k} \frac{HD(R_i, R_j)}{n} * 100 \tag{5}$$

On the other hand, uniformity of an n-bit PUF for an instance i measures the proportion of 1 and 0 bits of each response, $r_{i,l}$ is the l-th bit of the response for an instance i. It is defined as its Hamming weight percentage:

$$(Uniformity)_i = \frac{1}{n} \sum_{l=1}^{n} r_{i,l} * 100 \tag{6}$$

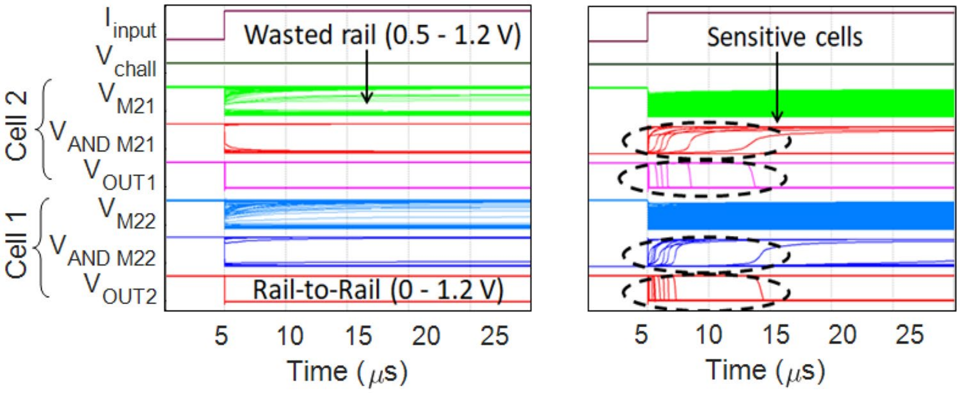
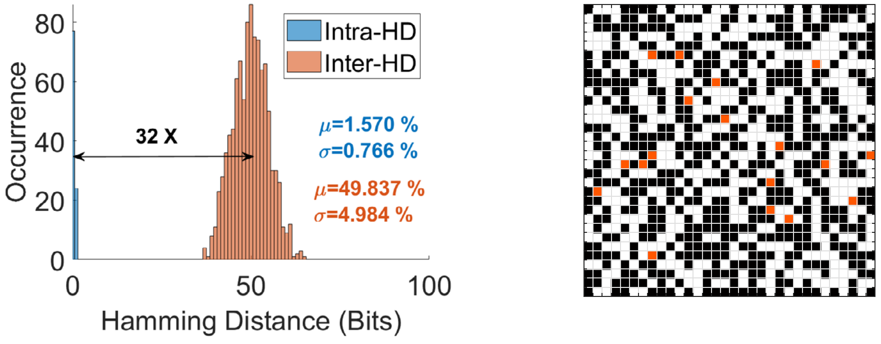


Fig. 10 Transistory behavior of the PUF cell. Secure and unsecure instance

Fig. 11 Inter and Intra PUF measurements



(a) Inter and intra HD

(b) PUF instance obtained at temperatures of -20, 60 and 120 C. Red color squares are unstable cells

Similarly, bit-aliasing allows to know if different chips may produce identical PUF responses which is an undesirable outcome. The bit-aliasing of the $l-th$ bit of the PUF is calculated as the percentage of Hamming weight for $l-th$ bit of PUF across k devices.

$$(Bit-aliasing)_l = \frac{1}{k}\sum_{i=1}^{k} r_{i,l} * 100, \tag{7}$$

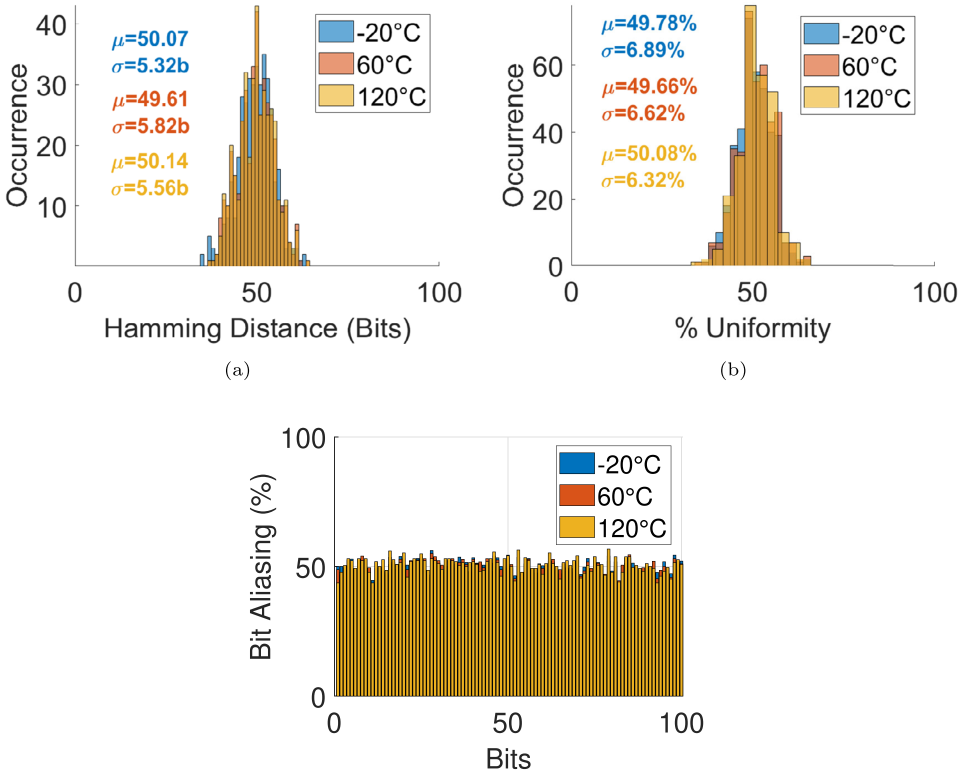
where $r_{i,l}$ is the $l-th$ binary bit of an $n-bit$ response for a chip i.

For 400 PUFs instances of 100 bits each, measurements of uniqueness, uniformity and bit aliasing were performed, Fig. 12 shows the results with statistical parameters for each temperature considered, (from measurements at different V_{DD} similar results are gotten but not displayed). From Fig. 12(a) and (b) it is emphasized that under any VT condition the bias of the PUF remains around 50%, and Fig. 12(c) shows that there are no bits biased at any conditions, the randomness and bit independence of the PUF is demonstrated.

4.3 Temperature and Voltage Variations

The variations in temperature and voltage of the PUF are quantified using the Hamming weight (HW) for the same 32 x 32 array (1024 bits) used in Subsection 4.1. To do this,

Fig. 12 Study on the impact of temperature on main PUF metrics, **a** Uniqueness **b** Uniformity **c** BitAliasing per bit

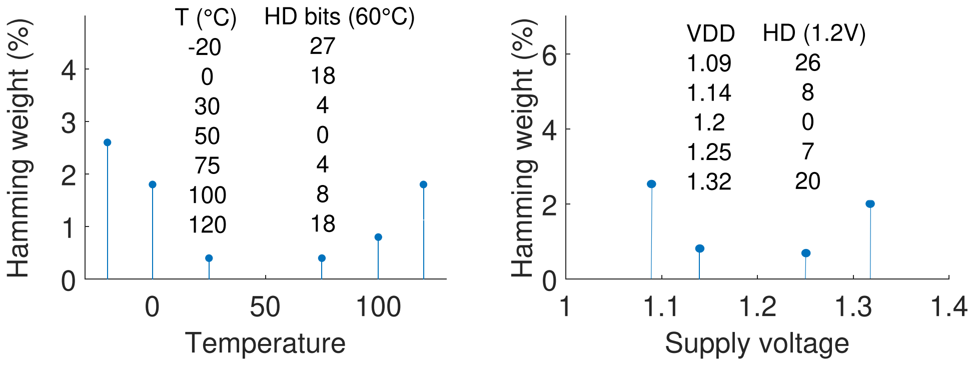


(a)

(b)

(c)

Fig. 13 Measurements of native bit instability against temperature and voltage variations



(a) Temperature native bit instability

(b) Voltage native bit instability

a nominal response is obtained and used as a reference to be compared against responses affected due to variations Fig. 13. Then the percentage of HW and the number of bits are calculated. For temperature, the nominal value is 60 celsius, the response is obtained for each variation, the results are in the table in Fig. 13(a). The process is similar for voltage variations, where the nominal 1.2V of the technology is used Fig. 13(b). The total native bit instability considering temperature and voltage variations is 2.294%. These results show that as PUF's operating conditions move away from the nominal, there is an increase in the HW. It is important to keep the native instability percentage as low as possible, so that, the use of additional hardware such as base cells or post-processing for BER reduction can be avoided.

4.4 Unpredictability Validation with NIST and ACF tests

True unpredictability of the PUF is verified through NIST and ACF. NIST tests are performed in Table 1, due to this limited data tests named non-overlapping template and universal statistical were not possible to run; all the other validation NIST were successful. A white noise bit stream must have an ACF mean value close to zero at 95% confidence level. In Fig. 14, the ACF for 10000 bits (100b x 100PUF) presents statistical values of $\mu = -1.2848 * 10^{-5}$ and $\sigma = 0.0032$ at the confidence level of ± 0.006, these results are remarkable prove the PUF random unpredictability and capability of resilience under autocorrealtion attacks.

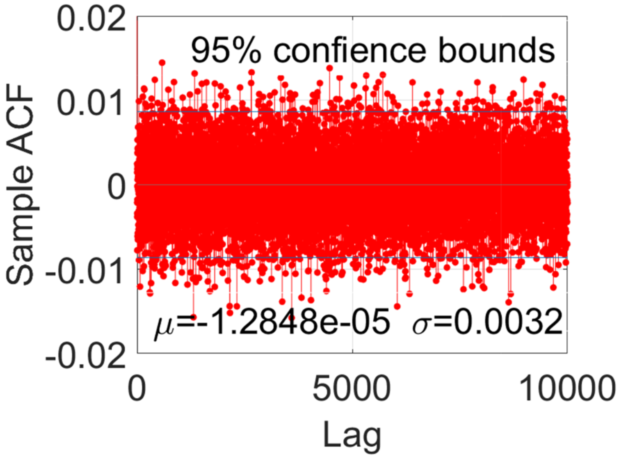


Fig. 14 Autocorrelation function (ACF) of 10000 bits generated

4.5 Comparison with the State of the Art

In Table 2, the comparison between this work and the state-of-the-art in CMOS technology is evident. The sources of entropy differ for the majority of works. The percentage of native unstable bits is a metric that, when addressed from the PUF circuit design perspective, can lead to a reduction in the required resources to improve the BER. For this work, all unstable bits are due to voltage and temperature variations, so temporal and spatial run-time stabilization techniques (SMV/TMV) will not be required to improve the BER. The proposed PUF achieves good performance metrics and

Table 1 NIST test performed over the PUF responses

P-VALUES AND THE PROPORTION OF PASSING SEQUENCES			
P-VALUE	PROPORTION	STATISTICAL TEST	PASS?
0.014551	59/59	Frequency	YES
0.001030	57/59	BlockFrequency	YES
0.037566	58/59	CumulativeSums	YES
0.401199	59/59	Runs	YES
0.012650	59/59	LongestRun	YES
0.693720	59/59	Rank	YES
0.286321	59/59	FFT	YES
/	55/59	NonOverlappingTemplate	/
0.886589	59/59	OverlappingTemplate	YES
/	59/59	Universal	/
0.152172	59/59	ApproximateEntropy	YES
0.102526	58/59	Serial	YES
0.631643	54/59	LinearComplexity	YES

Table 2 Performance comparison with state of the art

	[12]	[16]	[23]	[3]	[8]	[13]	**This work**
Technology	130*nm*	14*nm*	65*nm*	28*nm*	12*nm*	40*nm*	**65nm**
PUF type	SRAM mismatch (HCI reinforcement)	Delay hardened hybrid cell	WTA cell comparison	NAND gate mismatch	Pre amplifier	Delay (Ring Oscillator)	**Current mirror mismatch, WTA cells**
Area/bit	$497F^2$	$9388F^2$	—	$3699F^2$	$9954um^2$	$13220F^2$	**$1106um^2$**
Native unstable bits	2.71%	26.37%	12.07%	≈ 25%	9.32%	11% - 0.88%	**2.29%**
Temperature range (C)	-40 - 120	25 - 110	-20 - 100	-40 - 150	-40 - 125	-40 - 125	**-20 - 120**
VDD range	0.5 - 0.7	0.7 - 1.0	0.7 - 1.4	0.81 - 0.99	0.7 - 1	0.9 - 1.4	**1.08 - 1.32**
Inter HD	48.73%	48.6%	49.3%	≈ 49.78 %	49.60%	1044 inter-intra ratio	**49.84%**
Intra HD	0.41%	3.4%	—	—	1.6% 3.01%	48 %	**1.57%**
Energy/bit (fJ)	15.39	4	8920	2969	21	180	**5670**

examines the raw keys without any post-processing. If necessary, conventional techniques such as error correction codes or helper data algorithms can be applied to achieve even better results in metrics at the expense of increased global energy consumption.

5 Conclusion

A CMOS current mirror WTA based PUF was presented in this article, the basic cell proposed achieves high gain and a strong inhibition effect, both sensitive to mismatch and process variations which forces a random neuron to be the winner for all environmental conditions by consuming energy of $5.67pJ/b$. A PUF macro using an array of NxM cells creates an unique, unpredictable and low native bit instability footprint for each instance, able to produce strong PUF bits states in the vast majority of cases (97.706% of reliability), PUF true randomness was validated with NIST and ACF tests, with solid key generation latency of $73ns$ (8b) for nominal operation condition. As a result of this macro implementation, the PUF presented inter-HD and intra-HD measurements close to ideal values, a bit flipping rate of 2.142%. PUF metrics of uniqueness and uniformity were also valued close to ideal when environmental variations are considered.

Data Availibility The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

Declarations

Conflicts of Interest All authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript.

References

1. Atwady Y, Hammoudeh M (2017) A survey on authentication techniques for the internet of things. In: Proceedings of the International Conference on Future Networks and Distributed Systems
2. Chang C-H, Zheng Y, Zhang L (2017) A retrospective and a look forward: Fifteen years of physical unclonable function advancement. IEEE Circuits Syst Mag 17(3):32–62
3. Choi Y, Karpinskyy B, Ahn K-M, Kim Y, Kwon S, Park J, Lee Y, Noh M (2020) Physically unclonable function in 28nm fdsoi technology achieving high reliability for aec-q 100 grade 1 and iso 26262 asil-b. In: 2020 IEEE International Solid-State Circuits Conference-(ISSCC), pp. 426–428. IEEE
4. Dhar T, Trivedi A (2016) Area and energy-efficient physically unclonable function based on k-winners-take-all. Electron Lett 52(24):1978–1980
5. Gassend B, Clarke D, VanDijk M, Devadas S (2002) Silicon physical random functions. In: Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 148–160. ACM
6. Gunay ZS, Sanchez-Sinencio E (1997) Cmos winner-take-all circuits: a detailed comparison. In: 1997 IEEE International Symposium on Circuits and Systems (ISCAS) 1:41–44. IEEE
7. Huth C, Zibuschka J, Duplys P, Güneysu T (2015) Securing systems on the internet of things via physical properties of devices and communications. In: 2015 Annual IEEE Systems Conference (SysCon) Proceedings, pp. 8–13. IEEE
8. Hunt-Schroeder E, Xia T (2023) 12-nm stable pre-amplifier physical unclonable function with self-destruct capability. IEEE Transactions on Very Large Scale Integration (VLSI) Systems
9. Jeon D, Baek JH, Kim DK, Choi B-D (2015) Towards zero bit-error-rate physical unclonable function: Mismatch-based vs. physical-based approaches in standard cmos technology. In: 2015 Euromicro Conference on Digital System Design, pp. 407–414. IEEE
10. Kumar R, Patil VC, Kundu S (2012) On design of temperature invariant physically unclonable functions based on ring oscillators. In: 2012 IEEE Computer Society Annual Symposium on VLSI, pp. 165–170. IEEE
11. Lazzaro J, Ryckebusch S, Mahowald MA, Mead CA (1988) Winner-take-all networks of o (n) complexity
12. Liu K, Chen X, Pu H, Shinohara H (2020) A 0.5-v hybrid sram physically unclonable function using hot carrier injection burn-in for stability reinforcement. IEEE J Solid-State Circuits 56(7):2193–2204

13. Park J, Sim J-Y (2023) A reconfigurable ldo-assisted physically unclonable function achieving a zero-ber with 14% masking. Regular Papers, IEEE Transactions on Circuits and Systems I
14. Prinetto P, Roascio G (2020) Hardware security, vulnerabilities, and attacks: A comprehensive taxonomy. In: ITASEC, pp. 177–189
15. Rukhin A, Soto J, Nechvatal J, Smid M, Barker E (2001) A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, Booz-allen and hamilton inc mclean va
16. Satpathy S, Mathew SK, Suresh V, Anders MA, Kaul H, Agarwal A, Hsu SK, Chen G, Krishnamurthy RK, De VK (2017) A 4-fj/b delay-hardened physically unclonable function circuit with selective bit destabilization in 14-nm trigate cmos. IEEE J Solid State Circuits 52(4):940–949
17. Sekerkiran B, Cilingiroglu U (1998) Precision improvement in current-mode winner-take-all circuits using gain-boosted regulated-cascode cmos stages. In: 1998 IEEE International Joint Conference on Neural Networks Proceedings. IEEE World Congress on Computational Intelligence (Cat. No. 98CH36227) 1:553–556. IEEE
18. Shamsi K, Jin Y (2016) Security of emerging non-volatile memories: Attacks and defenses. In: 2016 IEEE 34th VLSI Test Symposium (VTS), pp. 1–4. IEEE
19. Shamsoshoara A, Korenda A, Afghah F, Zeadally S (2019) A survey on hardware-based security mechanisms for internet of things. arXiv preprint arXiv:1907.12525
20. Suh GE, Devadas S (2007) Physical unclonable functions for device authentication and secret key generation. In: 2007 44th ACM/IEEE Design Automation Conference, pp. 9–14. IEEE
21. Technology of Standards N.I. (2001) Security requirements for cryptographic modules. Technical Report Federal Information Processing Standards Publications (FIPS PUBS) 140-2, Change Notice 2 December 03, 2002, U.S. Department of Commerce, Washington, DC
22. Zhang J, Lin Y, Lyu Y, Qu G (2015) A puf-fsm binding scheme for fpga ip protection and pay-per-device licensing. IEEE Trans Inf Forensics Secur 10(6):1137–1150
23. Zheng W, Pan X, Zhao X (2019) A low power current mode puf based on winner-take-all scheme. In: 2019 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1–5. IEEE

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Joseph Herbert Mitchell-Moreno was born in San Andres Island, Colombia, he received the M. Sc. degree from the National Institute for Astrophysics, Optics and Electronics (INAOE), in 2019, where he is currently pursuing the Ph.D. degree. His research interests include mixed signal design systems, PUF design, analog design for security applications based on VLSI circuits and layout generation.

Guillermo Espinosa Flores-Verdad was born in Mexico City, he obtained the M. Sc. degree from INAOE, Mexico, and the Ph.D. degree from Pavia University, Italy in 1983 and 1989. From 1980 to 1985 he worked in the Electronic Engineering Dept. at the Autonomous University of Puebla, Mexico. From 1990 to 1993 he worked in the Central Research and Development Dept. at SGS- THOMSON Microelectronics Corp., Italy, as head of the Analog Library Automation Group. In February 1993, he joined the Electronics Dept. at the National Institute of Astrophysics, Optics and Electronics (INAOE), Mexico as a Professor Researcher. He was with Freescale Semiconductor from 2005 to 2008 leading the Freescale Mexico Technology Center. Since 2008, he is, again, at INAOE Electronics Department as a Professor Researcher. His main research interests are in Analog and Mixed Integrated Circuit Design and CAD development for the automatic design, synthesis, analysis and layout of ICs and Robust Design of Analog Integrated Circuits.