A $266F^2$ Ultra Stable Differential NOR-Structured Physically Unclonable Function With $< 6\times10^{-9}$ Bit Error Rate Through Efficient Redundancy Strategy

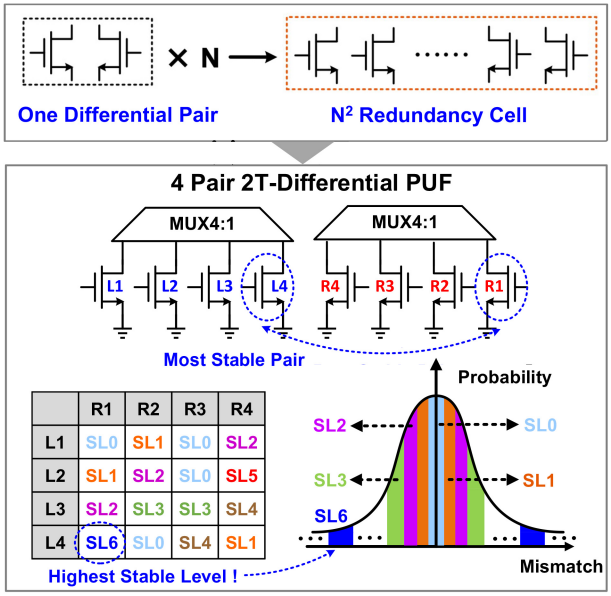
Haoyi Zhang, Jiahao Song, *Graduate Student Member, IEEE*, Haoyang Luo, *Graduate Student Member, IEEE*, Xiyuan Tang, *Senior Member, IEEE*, Yuan Wang, *Member, IEEE*, Runsheng Wang, *Member, IEEE*, and Ru Huang, *Fellow, IEEE*

***Abstract*—This brief presents a NOR-structured physically unclonable function (PUF) tailored for low-cost Internet of Things (IoT) applications. The proposed NOR-structured PUF utilizes a single minimum-sized differential NMOS pair, capitalizing on threshold-voltage mismatch as the entropy source. Fabricated in 65nm CMOS, the basic PUF cell is a $58F^2$ differential NMOS pair, demonstrating a raw bit error rate (BER) of 0.31%. To further enhance the stability and achieve an ultra-low BER, we introduce an area-efficient redundancy strategy. By incorporating 4x redundancy cells ($266F^2$ in total), the prototype chip achieves an ultra-low BER (zero error in 20M bits), over a wide temperature range (−20 to 125°C) and supply voltage variations (0.8 to 1.2V). The core energy consumption is only 63fJ/bit, offering a low-cost and highly stable solution for IoT applications.**

***Index Terms*—NOR-structured, physically unclonable function (PUF), redundancy strategy, ultra-low BER, low-cost.**

I. Introduction

PHYSICALLY unclonable function (PUF), which exploits the random process variation to generate unique challenge-response pairs (CRPs), have emerged as an attractive solution for edge authentication. Towards low-cost and secure Internet of Things (IoT) applications, the PUF circuits featuring ultra-low bit error rate (BER), low area, and low energy consumption are highly desirable. However, the state-of-the-art PUF designs face challenges in achieving ultra-low BER while maintaining low energy and area. Recent studies highlight two typical PUF structures: the ring-oscillator (RO)-based PUFs [1], [2] and NAND-structured PUFs [3], [4]. RO-based PUFs can achieve ultra-low BER ($<4.88\times10^{-6}$) under nominal voltage and temperature conditions (VT) [2]. However, the multi-stage RO and configuration block occupies a large area ($>20000F^2$). NAND-structured PUFs, on the other hand, are implemented with a small cell area of only $20F^2$ [3], [4]. Despite their compact size, they are vulnerable to noise due to insufficient cell-level mismatch amplification, thus requiring the power-hungry low-noise readout circuits (30nJ/bit). Additionally, their remapping and trimming strategies fail to achieve ultra-low BER.



	R1	R2	R3	R4
L1	SL0	SL1	SL0	SL2
L2	SL1	SL2	SL0	SL5
L3	SL2	SL3	SL3	SL4
L4	SL6	SL0	SL4	SL1

Fig. 1. The concept of redundancy PUF.

Intending to simultaneously achieve all desired properties of a PUF circuit, we propose a low-cost ultra-low BER ($<6\times10^{-9}$ BER at nominal VT) NOR-structured PUF cell with a redundancy strategy. While the output of a single minimum-sized differential NMOS pair may be unstable due to insufficient mismatch, combinations of a few unstable cells can generate sufficient redundancy pairs guaranteeing a stable output. Fabricated in 65nm CMOS, the basic NOR-structured PUF cell is a $66F^2$ differential NMOS pair with a raw BER of

Manuscript received 20 May 2024; revised 5 July 2024; accepted 22 July 2024. Date of publication 25 July 2024; date of current version 26 November 2024. This work was supported in part by the Joint Funds of the National Natural Science Foundation of China under Grant U20A20204 and Grant 62125401, and in part by the Beijing Natural Science Foundation under Grant L244051. This brief was recommended by Associate Editor A. Yan. *(Corresponding authors: Xiyuan Tang; Yuan Wang.)*

Haoyi Zhang, Jiahao Song, Yuan Wang, Runsheng Wang, and Ru Huang are with the School of Integrated Circuits, Peking University, Beijing 100871, China (e-mail: hy.zhang@stu.pku.edu.cn; wangyuan@pku.edu.cn; r.wang@pku.edu.cn).

Haoyang Luo and Xiyuan Tang are with the Institute for Artificial Intelligence, and the School of Integrated Circuits, Peking University, Beijing 100871, China (e-mail: xitang@pku.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCSII.2024.3433543.

Digital Object Identifier 10.1109/TCSII.2024.3433543

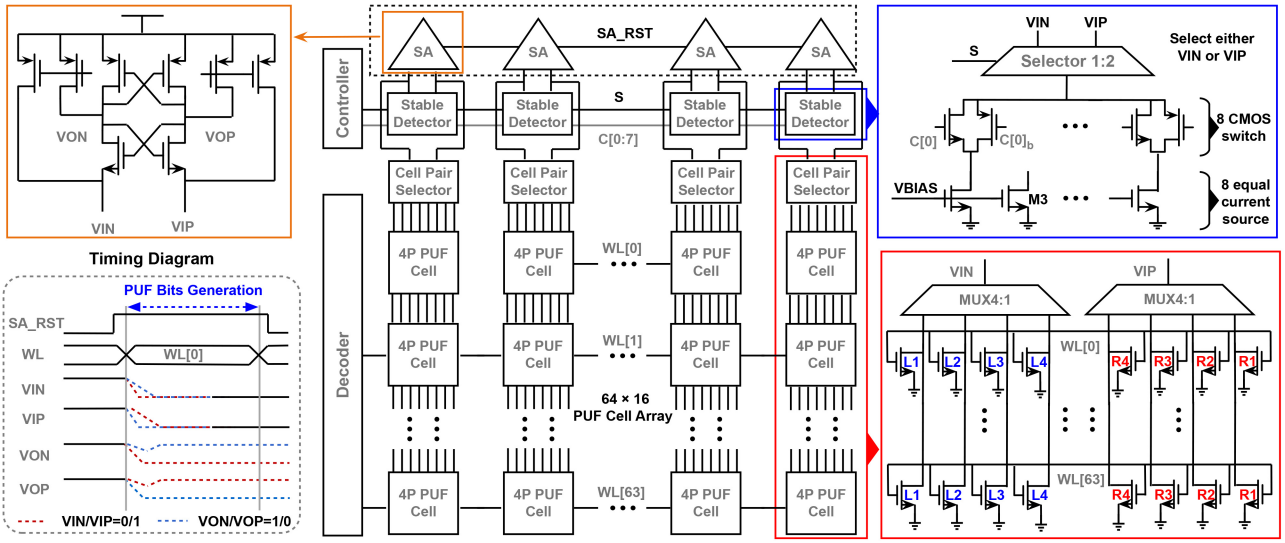


Fig. 2. The overall architecture, detailed circuit, and timing diagram of the proposed redundancy PUF.

0.31%. The high-quality basic PUF cell forms the foundation of the redundancy strategy. With 4× redundancy cells ($266F^2$ in total), the prototype chip achieves ultra-low BER (zero errors in 20M bits) across a wide temperature range (−20 to 125°C) and supply voltage variations (0.8 to 1.2V). The core energy consumption is only 63fJ/bit, demonstrating a low-cost and robust solution for secure IoT applications.

II. Proposed Circuit

Figure 1 illustrates the design principle of the proposed redundancy-based PUF. The intuitive idea of this brief is to select the most stable pair from different combinations. The most stable pair has the strongest resistance to mismatch and can reach the highest stable level. This innovative approach distinguishes itself from traditional PUF architectures by achieving a commendable equilibrium among BER, area, and energy consumption, which are critical metrics in PUF design. At the core of this design is the redundancy cell, which is composed of 2×N transistors, where N represents the number of differential pairs. Remarkably, this configuration allows for the generation of N^2 valid transistor pairs through various combinations. Within this array of combinations, it is sufficient for just one pair to exhibit enough mismatch to counteract VT variations and offset issues in the comparators. This feature underscores a notable trade-off: while increasing redundancy enhances the stability of the PUF, thus easing the demands on comparator precision, it also leads to a proportional increase in area consumption.

In practical terms, the implementation of this redundancy cell in silicon includes 8 minimum-sized transistors (corresponding to N = 4, yielding 16 redundancy pairs) and occupies an area of $266F^2$. This compact and efficient design is capable of consistently generating one stable pair, even under a broad range of operational conditions, spanning VT variations from −20 to 125°C and supply voltages from 0.8 to 1.2V.

Contrary to the spatial majority voting (SMV) scheme, where all PUF bits within a group must be read out as discussed by Song et al. [5], the redundancy approach requires access to only the selected pair within a cell. This selective access significantly reduces power consumption, offering a substantial advantage in terms of energy efficiency. Overall, the redundancy strategy greatly enhances the stability of the PUF while incurring only a tolerable increase in area overhead. This makes it an attractive solution for applications requiring high reliability and security in variable operational environments.

Figure 2 illustrates the circuit diagram and timing waveforms of the proposed redundancy PUF, which comprises an array of 64×16 PUF cells. While NAND-structured PUFs are known for their high area efficiency, they suffer from significant power overhead due to the large parasitic capacitance on the bit lines. To mitigate this issue, the proposed design employs a NOR-structured array, which strikes a better balance between area overhead and energy efficiency. Each PUF cell in this design contains eight transistors, divided equally into left and right groups. This symmetrical arrangement ensures that the design maintains balance and minimizes mismatch. During each read evaluation cycle, two analog multiplexers (MUXs) are used to select specific pairs within a column for evaluation.

The operation of the PUF is divided into two main phases: the reset phase and the bit generation phase. During the reset phase (when CLK = 0), the nodes VIN/VIP and VON/VOP are pre-charged to the supply voltage VDD. This pre-charging step ensures that all nodes start from a known, stable state, which is crucial for reliable operation. When the PUF bit generation phase begins (when CLK = 1), the clock signal transitions to high. At this point, the sense amplifier (SA) latch structure is activated. The SA latch forms a positive feedback loop, which amplifies any mismatch between the selected differential pair. This amplification is critical, as it ensures that even small mismatches due to process variations are detected and result in a stable PUF bit.

The use of a NOR-structured array significantly reduces the parasitic capacitance compared to a NAND structure, thereby

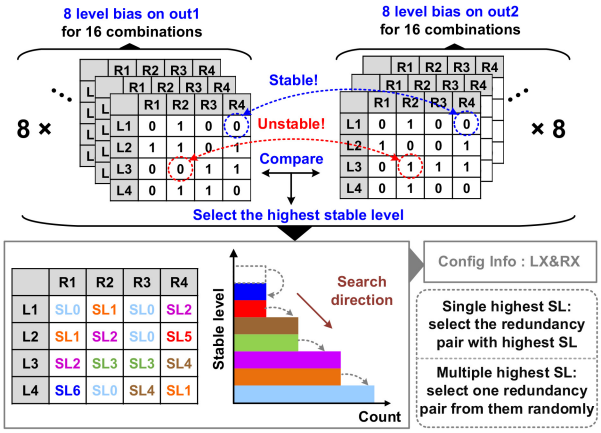


Fig. 3. Overview of the redundancy strategy.

TABLE I
NIST PUB 800-22 RESULTS

NIST Pub 800-22	Raw Data (Stream Length=1024)		Stabilized Data (Stream Length=1024)	
Test name	Avg. P-value	Pass Rate	Avg. P-value	Pass Rate
Frequency	0.48	100%	0.36	100%
Block Frequency	0.43	100%	0.39	100%
Runs	0.44	100%	0.41	100%
Longest Runs	0.32	100%	0.53	100%
Cumulative Sums	0.34	100%	0.32	100%
FFT	0.52	100%	0.37	100%
Non-overlapping Templates	0.83	100%	0.63	100%
Serial	0.37	100%	0.42	100%
Approximate Entropy	0.48	100%	0.46	100%

decreasing the power consumption. The careful design of the PUF cells, with eight transistors divided into two groups, enhances the stability of the generated bits by minimizing the impact of threshold voltage variations and comparator offsets. Moreover, this redundancy strategy only requires accessing the selected pair in a redundancy cell, unlike the spatial majority voting (SMV) scheme where all PUF bits in the group need to be read out. This selective access leads to significant power savings and improves the overall energy efficiency of the PUF.

In addition to the fundamental NOR-structured PUF array, the effective implementation of redundancy strategies is essential to significantly enhance both performance and reliability. A critical requirement for this implementation is the precise estimation of the stable level for each redundancy pair. Achieving fine-grained stable level separation demands accurate perturbation, which is why current sources are employed. These current sources are chosen for their precision and stability, ensuring reliable measurements.

For each column in the PUF array, eight current sources are used to generate the necessary currents. These currents are then selectively injected into either the VIN or VIP terminals, as determined by the control signal S. This selective injection mechanism ensures that each PUF cell operates under well-defined and controlled conditions. Consequently, this allows for accurate stability measurements and the determination of the most stable redundancy pairs.

The redundancy strategy and the specifics of stable level determination are illustrated in Fig. 3. Each Physically Unclonable Function (PUF) cell can form a total of 16 different combinations. For each combination, eight levels (SL0 SL7) of current bias are injected into the opposite outputs. These outcomes are then compared to determine the stability of each combination. It is not always possible to reach the highest level of SL7 in a specific pair of PUF cell, for example, this PUF cell shown in Fig. 3 can only tolerate up to SL6 level of current bias. It should be noted that such complete comparison only needs to be done once for each chip in the testing. The overhead caused by dark bit detection will not impact the following testing procedure.

In more detail, for each of the 16 possible combinations of a PUF cell, we inject current biases of varying levels into the opposite outputs. The results from these combinations are analyzed by comparing the outcomes under opposite current biases at the same perturbation level. If the outcomes under these opposite biases are consistent, it indicates that the combination is stable at that specific level of perturbation. Among all the combinations for a given PUF cell, the one that demonstrates the highest stable level is selected as the final, optimal pair. In cases where multiple combinations achieve the same level of stability, a random selection process is employed to ensure fairness and avoid bias. It is important to note that this selection and evaluation process is conducted only once during the initialization phase of the system.

By performing this stability assessment during initialization, we ensure that the PUF cell operates at its most stable configuration throughout its usage. This approach minimizes the risk of errors and enhances the reliability of the PUF cell, making it a robust component in secure systems.

III. MEASUREMENT RESULTS

The measured Unstable Bit Rate (UBR) and Bit Error Rate (BER) for eight chips are presented in Fig. 4. With the application of the TMV 11 stabilization technique, the BER at nominal threshold voltage (VT) conditions (1.0V, 25°C) is significantly reduced from 0.29% to 0.15%. Similarly, the UBR at nominal VT conditions is decreased from 2.74% to 1.35%. The implementation of the proposed redundancy strategy further achieves an ultra-low BER across 20,000 evolutions for the eight chips at nominal VT.

To validate the robustness of the design, BER measurements were conducted over a wide range of temperatures (−20 to 125°C) and supply voltages (0.8V to 1.2V). Even under the worst-case scenarios, such as 1.0V at 125°C and 0.8V at 25°C, the ultra-low BER is maintained over 20,000 evolutions for a single chip, thanks to the low-cost redundancy PUF design. Fig. 5 details the BER and UBR variations among different chips. The minimal variations among the chips demonstrate the robustness and reliability of our design methodology.

Further evaluations were conducted to assess the randomness and uniqueness of the proposed PUF. As shown in Table I, a NIST 800-22 randomness test was performed on both the raw and stabilized data from the eight chips. The

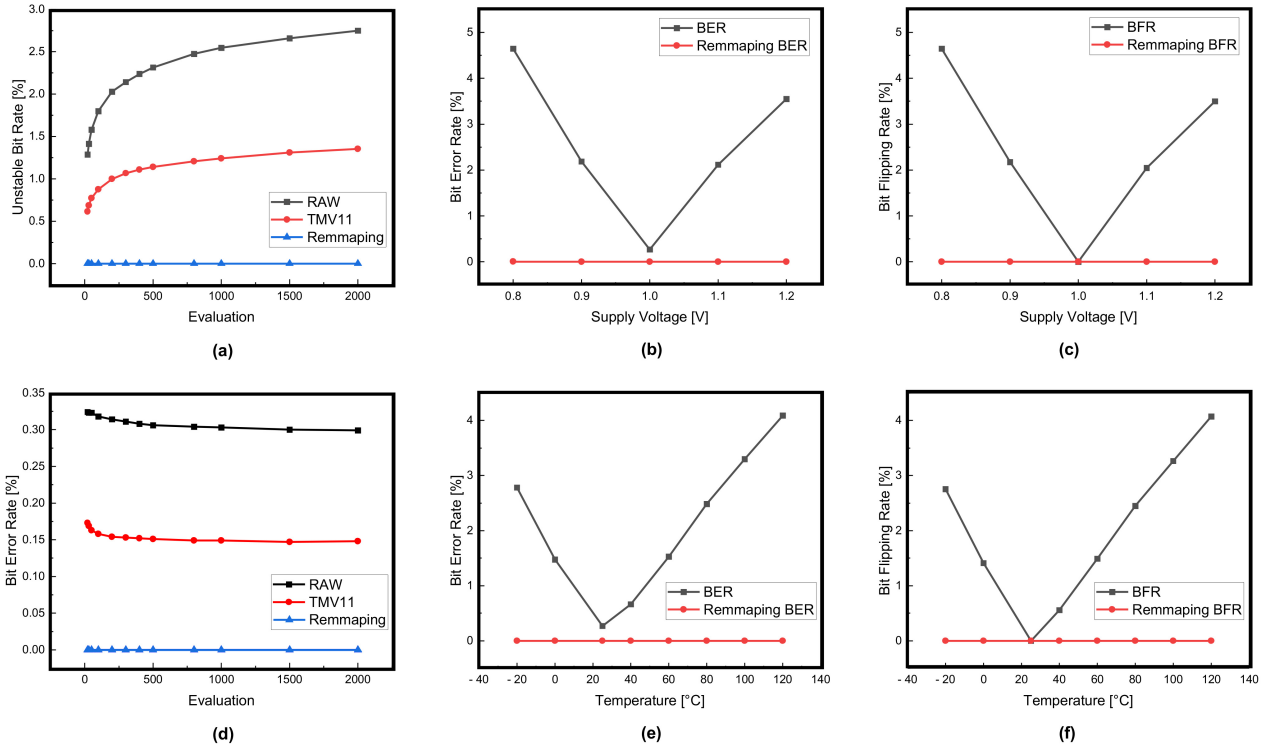


Fig. 4. (a) BER and (b) UBR versus number of evaluations. BER and BFR versus supply voltage ((c) and (d)) and temperature ((e) and (f)).

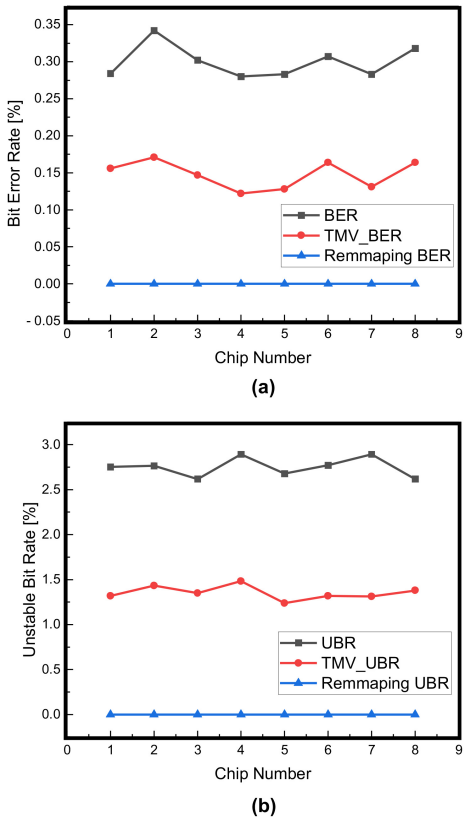


Fig. 5. BER and BFR versus among different chips.

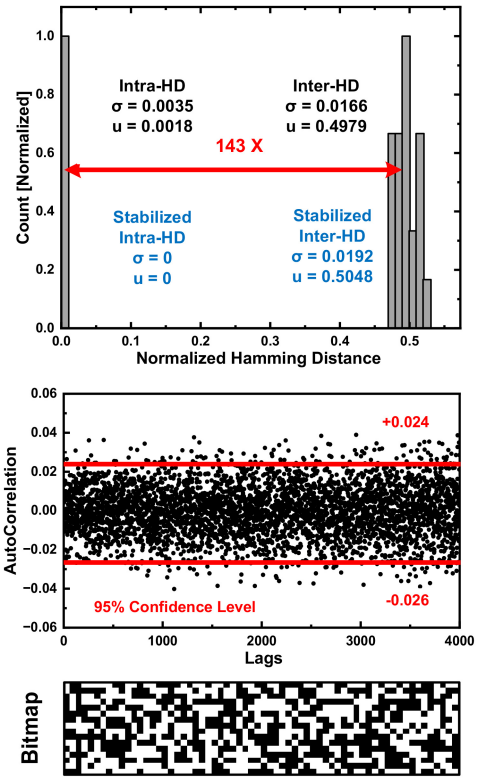


Fig. 6. (a) Inter-/intra-die HD, (b) auto-correlation, and (c) bitmap of the native data (measured at 1.2V supply voltage and 27°C).

raw data was generated under default conditions, selecting the L1 and R1 pairs from each PUF cell. All eight chips passed the test, confirming the inherent randomness of the design. Additionally, autocorrelation tests were conducted on the collection of data from the eight chips, totaling $8\times1024=8192$ bits. The results, including the normalized Hamming distance

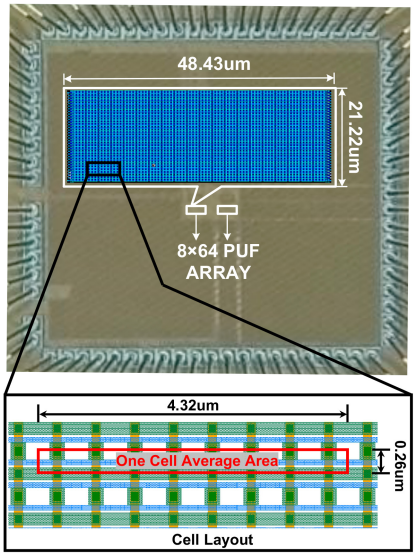


Fig. 7. Die photo and layout of PUF bit cells.

TABLE II
COMPARISON WITH SOTA WORKS

		This work	JSSC'22 [4]	TCAS II'24 [8]	JSSC'23 [6]	JSSC'20 [7]	JSSC'22 [2]
Technology		65nm	180nm	40nm	65nm	180nm	40nm
PUF Type		Current Integrated Differential-NOR	Current Integrated Differential-NAND	Leakage-based	Inverter Chain	EE SRAM	Ring-Oscillator
Stabilization Method		Redundancy	Remapping & Trimming	BCS	S-ASCH & D-ASCH	Dark Bit Detection & Mask	TMV7 & Mask
PUF Cell Area(F^2/Bit)		266[1]	20	982	594	373	21675
Native UBR (evaluations)		2.74% (2000)	7.85% (2000)	4.72% (2000)	3.20% (2000)	2.14% (2000)	0.20% (2000)
Native BER		0.29%	0.79%	0.48%	0.29%	0.21%	0.027%
Stabilized UBR		~0	0.64%	/	~0	~0	~0
Stabilized BER		~0 (<6.10E-9)	0.088%	0.0053%	~0 (<1.77E-9)	~0 (<5.99E-7)	~0 (<4.88E-6)
Test condition	VDD(V)	0.8-1.2	1.5-1.9	0.75-1.5	0.7-1.4	1.0-1.8	0.7-1.4
	Temp(℃)	-20-125	-20-80	-50-125	-40-125	0-80	-40-125
Worst condition	BER before stabilization	4.64%	4.29%	6.90%	4.20%	5.82%	/
	BER after stabilization	~0 (<4.88E-8)[3]	0.61%	0.0053%	~0 (<1.77E-9)	~0 (<5.99E-7)	0.19%
PUF energy (pJ/Bit)		0.063	168	0.073	5.7E-5	0.128	0.039

[1]266F^2 is the core area of 4 pair PUF cell
[2]BER is tested on 8 chips with 20000 evolutions reading of 64×16 bits array
[3]BER is tested on 8 chips with 20000 evolutions reading of 64×16 bits array

(HD), autocorrelation analysis, and bitmap representations, are depicted in Fig. 6.

The die photo and layout provided in Fig. 7 offer a tangible view of the physical implementation of the PUF cells. The stabilization technique notably enhances the normalized HD performance, and the bitmap visually demonstrates the intuitive randomness of the stabilized PUF cell. The cell layout, featuring a source-drain shared connection, highlights the low-area implementation of the PUF cell. This efficient layout is crucial for integrating PUFs into space-constrained environments, such as IoT devices and other miniaturized electronics. Comparing the proposed design with some state-of-the-art PUFs [2], [3], [4], [6], [7], [8], [9], [10], as summarized in Table II, highlights the advancements made in reducing both area and energy consumption while maintaining or improving performance metrics. The proposed redundancy PUF achieves an ultra-low BER with an area of only 266F^2/bit and energy consumption of 63fJ/bit, demonstrating superior area and energy efficiency compared to existing solutions.

IV. CONCLUSION

This brief proposes an ultra-low BER (zero error in 20M bits) PUF based on a redundancy strategy with wide ranges of temperature (−20 to 125°C) and supply voltage (0.8 to 1.2V), demonstrating a robust solution for secure application. Fabricated in 65nm process, the proposed ultra-low BER PUF generated a key bit with only 266F^2 and 63fJ leveraging the stabilization method (redundancy strategy). The ultra-low BER can be achieved across a voltage range of 0.8-1.2 and a temperature range of −20-125°C as the measurement results demonstrate, satisfying the IoT application requirements under versatile scenarios.

REFERENCES

[1] Z.-Y. Liang, H.-H. Wei, and T.-T. Liu, "A wide-range variation-resilient physically unclonable function in 28 nm," *IEEE J. Solid-State Circuits*, vol. 55, no. 3, pp. 817–825, Mar. 2020.
[2] J. Park, B. Kim, and J.-Y. Sim, "A BER-suppressed PUF with an amplification of process mismatch effect in an oscillator collapse topology," *IEEE J. Solid-State Circuits*, vol. 57, no. 7, pp. 2208–2219, Jul. 2022.
[3] J. Lee, M. Kim, G. Shin, and Y. Lee, "A 20F ^{2} area-efficient differential NAND-structured physically unclonable function for low-cost IoT security," *IEEE Solid-State Circuits Lett.*, vol. 2, no. 9, pp. 139–142, Sep. 2019.
[4] J. Lee, M. Kim, M. Jeong, G. Shin, and Y. Lee, "A 20F ^{2} /bit current-integration-based differential NAND-structured PUF for stable and *V* / *T* variation-tolerant low-cost IoT security," *IEEE J. Solid-State Circuits*, vol. 57, no. 10, pp. 2957–2968, Oct. 2022.
[5] J. Song et al., "A 3T eDRAM in-memory physically Unclonable function with spatial majority voting Stabilization," *IEEE Solid-State Circuits Lett.*, vol. 5, pp. 58–61, Mar. 2022.
[6] Y. He, D. Li, Z. Yu, and K. Yang, "ASCH-PUF: A 'zero' bit error rate CMOS physically unclonable function with dual-mode low-cost stabilization," *IEEE J. Solid-State Circuits*, vol. 58, no. 7, pp. 2087–2097, Jul. 2023.
[7] K. Liu, Y. Min, X. Yang, H. Sun, and H. Shinohara, "A 373-F^2 0.21%-native-BER EE SRAM physically Unclonable function with 2-D power-gated bit cells and VSS bias-based dark-bit detection," *IEEE J. Solid-State Circuits*, vol. 55, no. 6, pp. 1719–1732, Jun. 2020.
[8] L. Ni et al., "SI PUF: An SRAM and inverter-based PUF with a bit error rate of 0.0053% and 0.073/0.042 pJ/bit," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 71, no. 4, pp. 2339–2343, Apr. 2024.
[9] X. Xue et al., "A 28nm 512Kb adjacent 2T2R RRAM PUF with interleaved cell mirroring and self-adaptive splitting for extremely low bit error rate of cryptographic key," in *Proc. IEEE Asian Solid-State Circuits Conf. (A-SSCC)*, 2019, pp. 29–32.
[10] J. Yang et al., "A novel PUF using stochastic short-term memory time of oxide-based RRAM for embedded applications," in *Proc. IEEE Int. Electron Devices Meeting (IEDM)*, 2020, pp. 39.2.1–39.2.4.