IUST
Iran University of Science and Technology

Iranian Journal of Electrical and Electronic Engineering

Journal Homepage: ijeee.iust.ac.ir

Pure Magnetic Memory-Based PUFs: A Secure and Lightweight Solution for IoT Devices

M. Akbari*, S. Mirzakuchaki*(C.A.), M. Fazeli**, M.R. Tarihi***

Abstract: In light of the growing prevalence of Internet of Things (IoT) devices, it has become essential to incorporate cryptographic protection techniques for high-security applications. Since IoT devices are resource-constraints in terms of power and area, finding cost-effective ways to enhance their security is necessary. Physical unclonable function (PUF) is considered a trusted hardware security mechanism that generates true and intrinsic randomness by extracting the inherent process variations of circuits. In this paper, a novel pure magnetic memory-based PUF is presented. The fundamental building blocks of the proposed PUF design are magnetic devices, the so-called mCells. These magnetoresistive devices exclusively utilize Magnetic Tunnel Junction (MTJ) components. Using purely MTJ in the main memory and sense amplifier in the proposed PUF leads to high randomness, high reliability, low power, and ultra-compact occupation area. The Monte Carlo HSPICE simulation results demonstrate that the proposed PUF achieves a uniqueness of 49.89%, uniformity of 50.02 %, power consumption of 1.43 µW, and an area occupation of 0.01 μm^2 per bit.

Keywords: Physically Unclonable Function (PUF), Magnetic Tunnel Junction (MTJ), non-Volatile Memory (NVM), Memory-based PUF.

1 Introduction

DUE Due to the proliferation of IoT applications, ensuring the security of such devices is critical to prevent data leakages and protect sensitive information. In order to make critical devices like wearable health monitoring devices and smart cards effectively immune against potential attacks from adversaries, it is essential to employ cryptographic protection for high-level security.

Using a physical unclonable function (PUF) can be beneficial for small, low-power, and resource-constrained IoT devices requiring high levels of security. In recent years, the utilization of PUFs for security purposes has been widely considered due to their inherent and nonreproducible characteristics, which arise from the intrinsic process variations. This capability enables PUFs to extract secret keys, making them an attractive solution for enhancing security measures. Besides, PUFs can be used in various applications such as oblivious transfer (OT), bit commitment (BC), secure booting, device authentication, identification, etc.

A popular category of PUF is memory-based PUF [1-4]. Memory-based PUFs are becoming increasingly popular as a cost-efficient and highly secure method for protecting sensitive data and storing cryptographic keys [1, 3, 4]. Memory-based PUFs retrieve the random response from the process variation of the system memory cells. While this particular type of PUF is categorized as weak PUF due to its relatively limited CRP space, it can still serve as a valuable means to create a tamper-resistant

Iranian Journal of Electrical & Electronic Engineering, 2023.
Paper first received 18 Jun 2023 and accepted 04 Nov 2023.
* The authors are with the Department of Electrical Engineering, Iran University of Science and Technology, Tehran, 16846-13114, Iran.
E-mails: m_akbari93@yahoo.com, m_kuchaki@iust.ac.ir.
** The author is with the Department of Information Technology, Halmstad University, SE-301 18 Halmstad, Sweden.
E-mail: mahdi.fazeli@hh.se.
*** The author is with the Department of Information and Communication Technology, Niroo Research Institute (NRI), Tehran, 14665517, Iran.
E-mail: mtarihi@nri.ac.ir.
Corresponding Author: S. Mirzakuchaki.

and unclonable unique identification (UID) for devices. This UID can effectively replace less secure non-volatile memory storage solutions. Memory-based PUFs can take advantage of the main memory's entropy, allowing them to provide a PUF solution without requiring significant additional hardware.

Due to the limitations associated with scaling down complementary metal-oxide semiconductor (CMOS) technology, there is ongoing research to explore emerging nanoelectronic devices, such as non-volatile memory (NVM), as potential alternatives [5-9]. Emerging technologies have shown promising capabilities in generating abundant entropy and physical randomness. The spintronic device is currently regarded as the most promising choice for universal memory technology. This is attributed to its non-volatile nature, compatibility with CMOS processes, long lifespan, and high integration density, as confirmed by various studies [10-12].

In this paper, we propose a novel PUF architecture based on pure magnetic memory. Our proposed design utilizes mCell memory, a form of magnetoresistive memory that uses only Magnetic Tunnel Junction (MTJ) devices [13]. Therefore, the proposed PUF uses MTJ as the primary variation source.

Conventional memory-based PUFs rely on the characteristics of transistors as the primary sources of variation. As described in [14], the variations in the transistor parameters, such as threshold voltage (V_{TH}), width, length, and oxide thickness, show different variation rates under temperature and voltage variations. However, creating crossover points can flip the response under temperature and voltage variations, compromising the reliability of CMOS-based PUFs. In contrast to transistors, the investigation of the resistance values of 10 Magnetoresistive Tunnel Junctions (MTJs) under temperature and voltage changes in [14] revealed a more consistent behavior with the same variation rates. Based on the more consistent behavior exhibited by MTJs under temperature and voltage variations, it can be concluded that MTJs are a more reliable option than transistors as the main variation source. This paper introduces a novel pure magnetic memory-based PUF that leverages the intrinsic variability of the mCell devices.

The mechanism to generate the random numbers in the proposed design is based on comparing the resistance values of each two mCells in adjacent columns that are set to high-resistance state. This is due to the fact that the resistance of MTJs in the high resistance state shows higher intrinsic randomness than the resistance in the low-resistance state [15]. Therefore, by choosing one cell from each adjacent column and reading their resistance values using a differential readout scheme, random responses are obtained.

In addition, as mentioned above, since the MTJs have constant variation rates under environmental fluctuations, the differential read-out scheme which is a pure SR-latch in the proposed design can eliminate variations and then stabilize the responses.

One significant advantage of the proposed design is that unlike recently proposed memory-based Physical Unclonable Functions (PUFs), which used CMOS transistors, the proposed design solely utilizes Magnetic Tunnel Junctions (MTJs). As a result, the area occupied and power consumed by each bit cell are significantly reduced in comparison to these memory-based PUFs. The paper is organized as follows. Section 2 introduces a background for understanding PUF and mCell.

The main contributions of this paper can be summarized as follows:

- Proposing a pure magnetic memory-based PUF with a very small area of occupation memory cell compared to the other state-of-the-art memory-based PUFs.
- Using a pure magnetic nonvolatile latch with the differential structure as the sense amplifier to obtain very high reliability without utilizing any post-processing techniques.
- Comparing the proposed PUF with the other state-of-the-art memory-based PUFs.

The proposed PUF and the simulation results are described in Section 3 and Section 4, respectively. Section 5 concludes the paper.

2 Preliminaries

In this section, we present a short but comprehensive overview of PUF and pure magnetic memory's basic characteristics.

2.1 Physically Unclonable Function (PUF)

A Physical Unclonable Function (PUF) is a cryptographic function designed to capture the distinct physical characteristics of a device by extracting them from the inherent deep submicrometer variations that arise during the random manufacturing process. PUFs generate a response, or output, corresponding to a given challenge or input. These PUFs can be classified into two main types: "strong" and "weak." Strong PUFs can produce a larger number of challenge-response pairs (CRPs) compared to weak PUFs. In the case of strong PUFs, the number of CRPs exhibits an exponential relationship with the number of PUF instances, whereas weak PUFs demonstrate a linear

relationship. Notable examples of strong and weak PUFs include Arbiter PUF and memory-based PUF, respectively.

2.2 Review of Pure Magnetic Memory

The schematic of a pure magnetic memory [16] has been depicted in Fig. 1. As can be observed, the memory is based on a spintronic device called mCell [17].

As can be seen in Fig. 1, Three mCells are utilized to form each memory cell, wherein two mCells form a driving buffer, and the third mCell serves as data storage and transfers the data stored to the output in the reading phase.

Writing a memory cell involves setting the WWL(j)+ and WWL(j)- writing lines to V+ and V- values, respectively. It causes the current to flow through the writing path.

The process of writing into a memory cell is determined by the direction of the output current of the driving buffer. Writing ’0’ in a memory cell makes the pull-up resistor greater than the pulldown resistor.

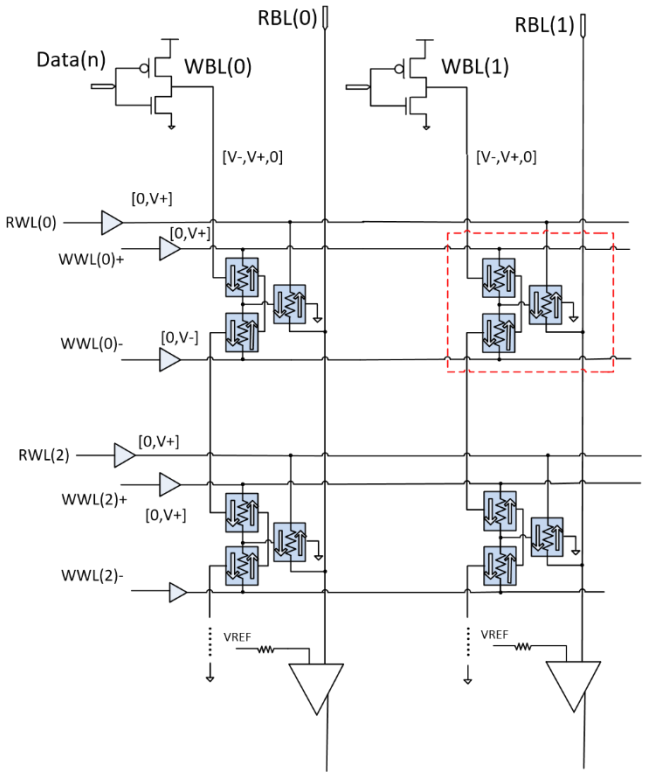


Fig. 1 2x2 Memory array of all magnetic devices. Peripheral elements.

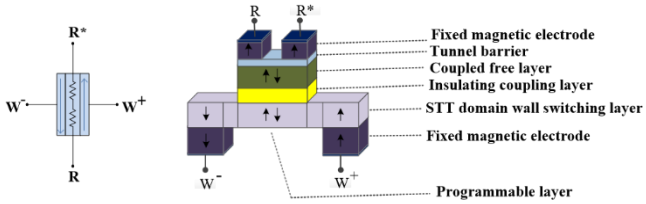


Fig. 2 mCell: (a) schematic symbol (b) 3-D view.

Therefore, by activating the WWL(j)+ and WWL(j)- lines, the output current of the driving buffer flows from left to right. In the case of writing ’1’ in a memory cell, the pull-down resistor becomes greater than the pull-down resistor and causes the direction of the output current of the driving buffer to be reversed.

Reading the stored data in a memory cell requires setting the RWL(i) line to V+, resulting in the flow of current through the BL(i). The read current of mCell can take on two values, '0' and '1', which correspond to the low resistor and high resistor states, respectively.

3 Proposed Pure Magnetic PUF

Fig. 3 shows the schematic of the proposed pure magnetic memory-based PUF. The circuit is composed of two parts; memory and comparator. The memory array is utilized to set the memory cells to the same state while the comparator is to generate the response based on the read-out difference in current values.

In order to generate random responses in our PUF solution, we make use of the intrinsic unpredictability and high variation of the resistance in antiparallel magnetization. This is because the MTJ resistance provides more variability when in an anti-parallel (AP) magnetization state than in a parallel (P) magnetization state, and this is due to both the intrinsic process of quantum tunneling and the extrinsic process of scattering. In digital circuits, the states of '0' and '1' are indicated by the resistance levels of R_P and R_{AP}, respectively.

The first step to generate random PUF responses is to set all the memory cells to '1' as was discussed in 2.2. According to the high variability in AP state, each two cells have a different resistance value which leads to different read currents in the read mode.

The next step involves reading the currently active cells that are stored in the memory array. This is achieved by asserting an appropriate RWL signal that makes a small current flow down into the read circuitry. Due to the fact that scratch buffers are actually inverters, small current and large currents being read correspond to logic-1 and logic-0 written to the bitcell, respectively. The RWL lines of each column are connected to a decoder. Depending on the

challenge bit, each row is connected to the high or zero voltage to be read.

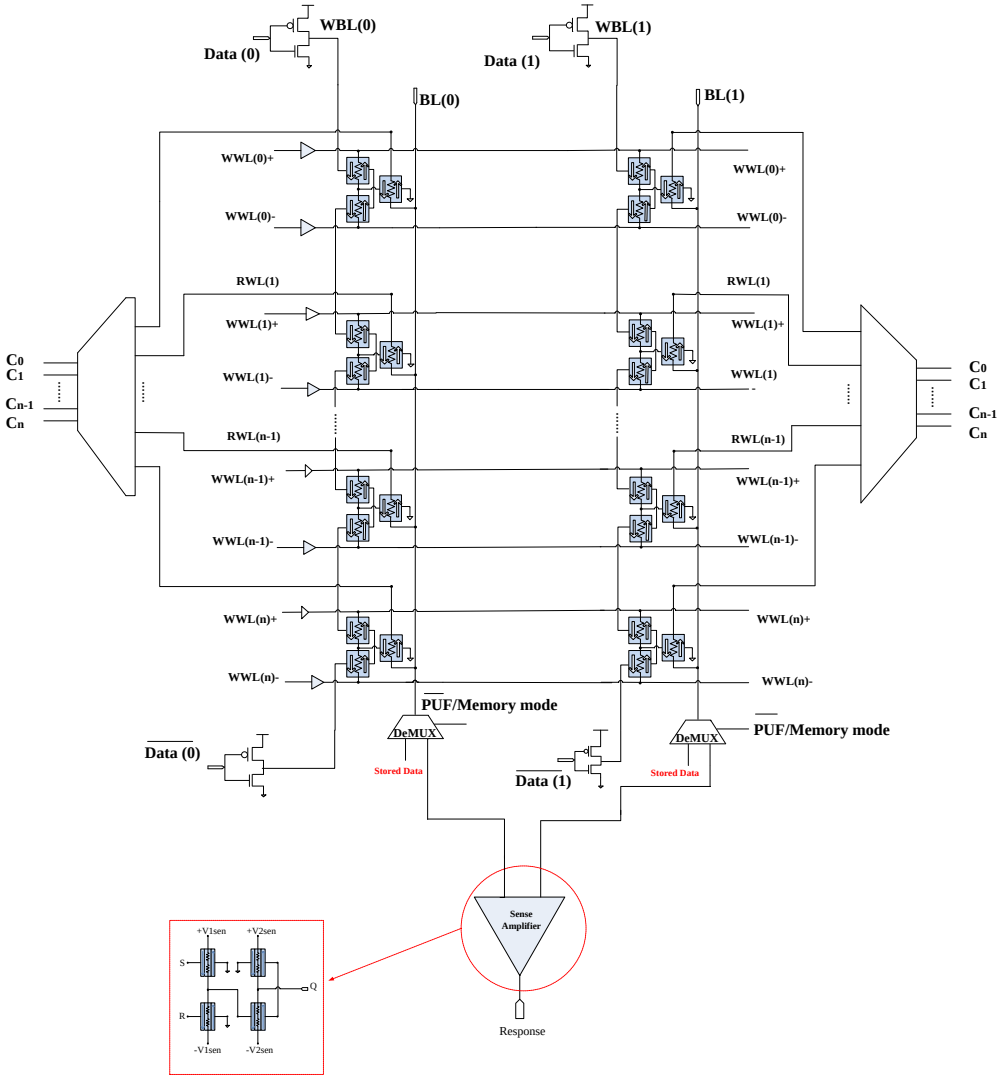


Fig. 3 The final configuration of proposed pure magnetic PUF.

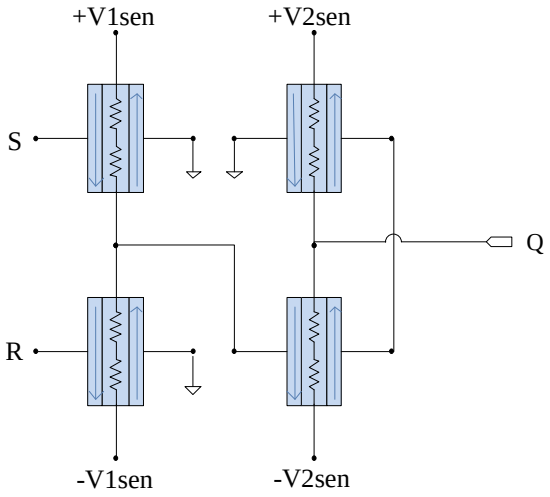


Fig. 4 The schematic of the pure magnetic non-volatile latch.

A DeMUX is located at the end of each WBL line to direct the write path current toward the SR latch or the sense amplifier based on whether the circuit is operating in PUF or memory mode. In memory mode the bitline of each column is connected to the sense amplifier to read the data stored in the memory whereas in PUF mode each two columns is connected to an SR latch. The mismatch of MTJ resistance values in each two cells is sensed to produce a random bit by using the SR latch.

As was discussed above MTJs in the same state exhibited similar variation rates under temperature and voltage variations. The differential structure of the SR latch enables it to eliminate environmental variations, resulting in increased reliability.

In this paper, a pure magnetic non-volatile latch is used as the arbiter to produce the result based on the difference of the current values. The schematic of the latch is depicted in Fig. 4(a). This latch consists of two parts. In this structure, the *S* and *R* inputs are directed to the initial part of the latch, which consists of two mCells. The latter part, also consist of two mCells, generates the *Q* output depending on the states of *S* and *R*. The corresponding truth table for this latch can be found in Table 1.

When a high signal is applied to the Set line of the latch, the upper mCell undergoes a transition to a high resistance state (R_H). Meanwhile, the bottom mCell remains unchanged, resulting in a positive difference between R_H and the resistance of the bottom mCell (R_L). As a result, the *Q* output becomes high. Conversely, if a high signal is applied to the Reset line while the Set line is in a '0' state, the bottom mCell switches to a high resistance state (R_H). This causes the difference between R_L and R_H to become negative, leading to a change in the *Q* output to low.

For the remaining two states, when both inputs are either high or low, the differences between R_L-R_L and R_H-R_H become zero. The truth table of the pure magnetic latch is depicted in Table 1.

Table 1 Truth table of the pure magnetic non-volatile latch.

S	R	mCell states		Q
0	0	R_L	R_L	No change
0	1	R_L	R_H	0
1	0	R_H	R_L	1
1	1	R_H	R_H	No change

4 Simulation Results

In this section, we demonstrate the simulation results of the proposed memory-based PUF. To evaluate the effectiveness of the Arbiter PUF (APUF), we conducted tests using 16-bit challenges and 32-bit output configurations. To this end, we replicated the single PUF cell shown in Fig. 3 n times to enable the generation of an n-bit response. In this section, various metrics such as uniqueness, uniformity, reliability, power consumption, and area as formulized in [18] are considered to provide a comprehensive analysis to assess the efficiency of the proposed PUF.

The circuit simulations were conducted utilizing Synopsys HSPICE using a developed Verilog-A model for the mCells as proposed in [19] at room temperature. The parameters employed in the

simulation of mCell elements have been taken from [17].

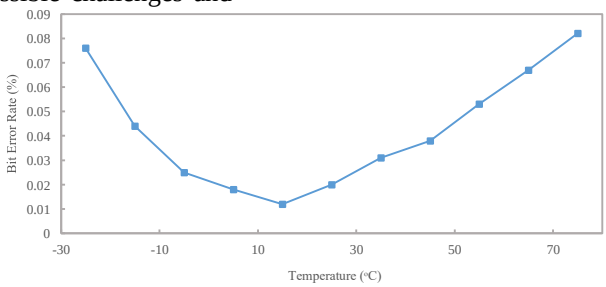
4.1 Bit Error Rate (BER)

This section evaluates the system's reliability performance under temperature and voltage variations using a metric called BER. It quantifies the extent to which environmental variations can influence the PUF response when the same challenges are applied repeatedly.

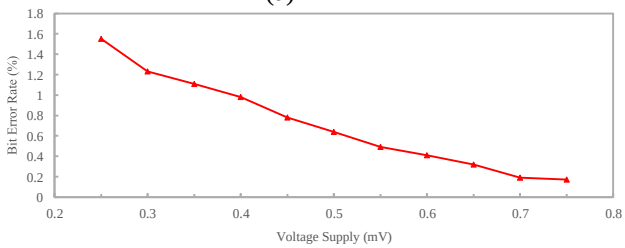
The BER value is determined by calculating the intra-chip Hamming distance, which measures the number of erroneous response bits obtained under temperature and voltage variations in a normal working environment. The operating temperature variation range is considered between -25 °C to 75 °C and the supply voltage variation range is considered between 25 mV to 75 mV. The PUF responses under these ranges are collected to calculate the BER. This metric should ideally be as low as possible, approaching 0%, for all the possible challenges and responses of the PUF. The BER under environment variations is obtained using the Eq. (1):

$$\mathrm{BER} = \frac{1}{k}\sum_{j=1}^{k}\frac{\mathrm{HD}(R_i\, R_{ij})}{n} \times 100\ \% \qquad (1)$$

where k is the number of applying the same challenge to the same PUF instance under different environmental conditions which leads to k responses (denoted as *Ri,j* for *j* = 1, 2, ..., *k*). The BER under temperature and voltage variation have been shown in Fig. 5(a) and Fig. 5(b), respectively. By changing the temperature, the worst-case BER is obtained as 0.08 %. Additionally, we have assessed the BER at different supply voltages. With 5 mV as the step, the BER is reported to be 0.76 %.



(a)



(b)

Fig. 5 BER over (a) Voltage variation, (b) Temperature variation.

4.2 Uniformity

The random behavior of a PUF response is conducted by measuring the proportion of 0's and 1's in the response bits. A security key that is difficult to duplicate is achieved by having an equal number of 1's and 0's distributed evenly. It is ideal for the distribution to be 50%. To assess the uniformity, the Hamming Weight (HW) is used, which is defined as [16] in Eq. (2):

$$(\mathrm{Uniformity})_i = \frac{1}{k}\sum_{j=1}^{k} r_{i,j} \times 100\ \% \qquad (2)$$

where $r_{i,j}$ denotes the *l*-th binary bit of an k-bit response originating from chip *i*.

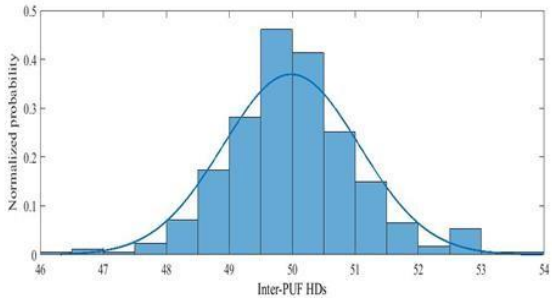


Fig. 6 The distribution of one 32-bit key in 1000 Monte Carlo simulations.

4.3 Uniqueness

Uniqueness is the metric used to determine how effectively one PUF instance can be distinguished from a set of similar PUFs. Typically, uniqueness is calculated as the mean of normalized inter-die Hamming distances (HDs).

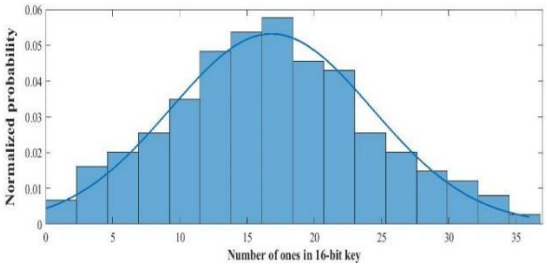


Fig. 7 The distribution of Hamming distances among 1000 pairs of inter-die for a 32-bit PUF, with 500 challenges.

These Hamming Distances (HDs) are determined through pairwise comparisons of the responses from a group of chips utilizing the same PUF design when subjected to an identical set of challenges. To ensure the uniqueness of PUFs, it is ideal for the inter-chip HD to be 50%.

Considering two chips, u and v, with n-bit responses Ru and Rv, respectively, to the same challenge C, the degree of uniqueness U for the m chips is then calculated in Eq. (3):

$$\text{Uniqueness} = \frac{2}{m(m-1)} \sum_{u=1}^{m-1} \sum_{v=u+1}^{m} \frac{HD(R_u R_v)}{n} \times 100\ \% \qquad (3)$$

5 Resource Consumption and Performance Comparison

Table 2 presents a comprehensive comparison between our proposed PUF and the recently reported implementations of a memory-based PUF.

By leveraging the valuable properties of MTJs, including their high density, compact size, and low power consumption, our proposed PUF demonstrates remarkable efficiency in terms of minimal area occupancy and power consumption per bit, surpassing other PUF implementations. The calculations reveal that the power consumption and area occupation for generating a single bit using the proposed PUF amount to merely 0.01 µm2 and 1.43 µW, respectively. Additionally, the inherent entropy provided by the MTJ contributes to the comparable levels of randomness and uniqueness achieved, with values of 50.02% and 48.98%, respectively.

Table 2 shows that the proposed PUF exhibits native Bit Error Rate (BER) values within the operational temperature range of -50°C to 150°C and supply voltage range of 25 mV to 75 mV. These BER values indicate that the proposed PUF is inherently reliable without the need for post-processing techniques that impose additional hardware and power overhead.

6 Conclusion

In this paper, we proposed a new design of memory-based PUF purely based on mCell devices. The high variability of mCell devices in HR is used to generate random responses by comparing the current flow from every two cells. Given the similar variation rates of MTJs under environmental variation, using a differential pure magnetic sense amplifier resulted in high reliability, the footprint, and the proposed pure magnetic arbiter PUF showcases remarkable characteristics. These include low power consumption, high reliability, high randomness, and an extremely compact design. eliminating the need for additional reliability-enhancement techniques. Due to the inherent properties of MTJs, such as nonvolatility, stochastic switching, chaotic magnetization, low power consumption, and compact subsystems, and satellite communications.

Table. 2 Performance comparison with the state-of-the-art memory-based PUF implementations**.**

Design		This work	PUF in [20]	PUF in [1]	PUF in [21]	PUF in [4]	PUF in [22]
Area per CRP (μm^2)		0.01	N/A	121	N/A	6.3	21.18
Maximum BER	Temperature	0.081	0.0017	3.51	N/A	0.21	4
	Supply voltage	0.76	0.0017	1.56	N/A	0.21	3
Temp. range (^{o} C)		-25∼ 75	-50∼ 100	-40∼ 120	N/A	-40∼ 120	0∼ 80
Supply volt. range (V)		0.25∼ 0.75	0.9∼ 1.1	1.2∼1.8	N/A	0.8∼ 1.4	0.5∼ 0.9
Power (μW/bit)		1.43	N/A	8.14	N/A	4.1	23.83
Randomness (%)		50.02	49.99	NIST (7/15)	50.54	NIST (15/15)	50
Uniqueness (%)		48.98	49.99	49.92	50.30	∼0.5	48.1-49.5
Reliability enhancement algorithm (%)		No	No	No	No	Yes Vss Bias Dark-bit detection	No

Reference

[1] Gan, P., X. Zhao, and Y. Cao, *An All-MOSFET Voltage Reference-Based PUF Featuring Low BER Sensitivity to VT Variations and 163 fJ/Bit in 180-nm CMOS.* IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2020. **40**(6): p. 1172-1182.

[2] Lim, S., B. Song, and S.-O. Jung, *Highly independent MTJ-based PUF system using diode-connected transistor and two-step postprocessing for improved response stability.* IEEE Transactions on Information Forensics and Security, 2020. **15**: p. 2798-2807.

[3] Pang, Y., et al., *Optimization of RRAM-based physical unclonable function with a novel differential read-out method.* IEEE Electron Device Letters, 2017. **38**(2): p. 168-171.

[4] Zhang, L., et al., *Optimizating emerging nonvolatile memories for dual-mode applications: Data storage and key generator.* IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015. **34**(7): p. 1176-1187.

[5] Chen, A., *A review of emerging non-volatile memory (NVM) technologies and applications.* SolidState Electronics, 2016. **125**: p. 25-38.

[6] Fong, S.W., C.M. Neumann, and H.-S.P. Wong, *Phase-change memory—Towards a storage-class memory.* IEEE Transactions on Electron Devices, 2017. **64**(11): p. 4374-4385.

[7] Konigsmark, S.C., L.K. Hwang, D. Chen, and M.D. Wong. *CNPUF: A carbon nanotube-based physically unclonable function for secure low-energy hardware design*. in *2014 19th Asia and South Pacific Design Automation Conference (ASP-DAC)*. 2014. IEEE.

[8] Cui, Y., et al., *Lightweight configurable ring oscillator PUF based on RRAM/CMOS hybrid circuits.* IEEE Open Journal of Nanotechnology, 2020. **1**: p. 128-134.

[9] Ghosh, S., *Spintronics and security: Prospects, vulnerabilities, attack models, and preventions.* Proceedings of the IEEE, 2016. **104**(10): p. 1864-1893.

[10] Iyengar, A.S., S. Ghosh, and K. Ramclam, *Domain wall magnets for embedded memory and hardware security.* IEEE journal on emerging

and selected topics in circuits and systems, 2015. **5**(1): p. 40-50.
[11] Iyengar, A., et al., *Spintronic PUFs for security, trust, and authentication.* ACM Journal on Emerging Technologies in Computing Systems (JETC), 2016. **13**(1): p. 1-15.
[12] Ghosh, S. and R. Govindaraj. *Spintronics for associative computation and hardware security*. in *2015 IEEE 58th International Midwest Symposium on Circuits and Systems (MWSCAS)*. 2015. IEEE.
[13] Prenat, G., et al. *CMOS/magnetic hybrid architectures*. in *2007 14th IEEE international conference on electronics, circuits and systems*. 2007. IEEE.
[14] Song, B., S. Lim, S.H. Kang, and S.-O. Jung, *Environmental-variation-tolerant magnetic tunnel junction-based physical unclonable function cell with auto write-back technique.* IEEE Transactions on Information Forensics and Security, 2021. 16: p. 2843-2853.
[15] Vatajelu, E.I., et al., *STT-MRAM-based PUF architecture exploiting magnetic tunnel junction fabrication-induced variability.* ACM Journal on Emerging Technologies in Computing Systems (JETC), 2016. **13**(1): p. 1-21.
[16] Bromberg, D., H. Sumbul, J.-G. Zhu, and L. Pileggi, *All-magnetic magnetoresistive random access memory based on four terminal mCell device.* Journal of Applied Physics, 2015. **117**(17): p. 17B510.
[17] Bromberg, D.M., D.H. Morris, L. Pileggi, and J.-G. Zhu, *Novel STT-MTJ device enabling all-metallic logic circuits.* IEEE transactions on Magnetics, 2012. **48**(11): p. 3215-3218.
[18] Maiti, A., R. Nagesh, A. Reddy, and P. Schaumont. *Physical unclonable function and true random number generator: a compact and scalable implementation*. in *Proceedings of the 19th ACM Great Lakes symposium on VLSI*. 2009.
[19] Bromberg, D.M., *Current-driven magnetic devices for non-volatile logic and memory*. 2014, Ph. D. dissertation, Carnegie Mellon Univ., Pittsburgh, PA, USA.
[20] Li, J., et al., *A Fully Configurable PUF Using Dynamic Variations of Resistive Crossbar Arrays.* IEEE Transactions on Nanotechnology, 2022. **21**: p. 737-746.
[21] Li, J., et al., *A physical unclonable function using a configurable tristate hybrid scheme with nonvolatile memory.* IEEE Open Journal of Nanotechnology, 2021. **2**: p. 31-40.
[22] Lim, S., et al. *A Highly Integrated Crosspoint Array Using Self-rectifying FTJ for Dual-mode Operations: CAM and PUF*. in *ESSCIRC 2022- IEEE 48th European Solid State Circuits Conference (ESSCIRC)*. 2022. IEEE.

MARYAM AKBARI was born in Kermanshah, Iran, in 1993. She received her B.Sc. and M.Sc. degrees from the Razi University, Iran, in 2015 and 2017, respectively. She is currently pursuing the Ph.D. degree at the Iran University of Science and Technology (IUST), Iran. Her research interests include microstrip filters, high-requency circuit design, Physical Unclonable Functions (PUFs), true random number generators, and emerging technologies.

SATTAR MIRZAKUCHAKI received the B.Sc. degree in Electrical Engineering from the University of Mississippi in 1989 and the M.Sc. and Ph.D. degrees in Electrical Engineering from the University of Missouri-Columbia in 1991 and 1996, respectively. He has been a faculty member of the School of Electrical Engineering at Iran University of Science and Technology, Tehran, since 1996. His current research interests include digital systems and design of VLSI circuits.

MAHDI FAZELI received his M.Sc and Ph.D. degrees in computer engineering both from Sharif University of Technology, Tehran, Iran, in 2005 and 2011, respectively. He is currently an associate professor at the School of Information Technology, Halmstad University, Sweden. His research interests include hardware security and trust, reliable VLSI circuits and systems, energy-efficient computing, and dependable embedded systems.

MOHAMMADREZA TARIHI was born in Iran in 1974. He received the B.Sc. and M.Sc. degrees in Electrical Engineering in 1997 and 2001, respectively, and received Ph.D. degree in Communication Engineering at Malek-e-Ashtar University of Technology (MUT), Tehran, Iran in 2019. From 2005 to 2014 he has been with the Electrical and Electronic Engineering University Complex (EEEUC), MUT, Tehran, Iran. Since 2014, he was a faculty of Niroo Research Institute (NRI), in Tehran, Iran. His research areas include broadband wireless communications, Cooperative communications, MIMO Systems, Microwave and Wireless Subsystems, and Satellite communications.