AUT Journal of Electrical Engineering

AUT J. Elec. Eng., 57(1) (2025) 31-42
DOI: 10.22060/eej.2024.22989.5578

Efficient and Lightweight IoT Security Using CNTFET-Based Ultra-Low Power SRAM-PUF

Alireza Shafiei, Mehrnaz Monajati*

Department of Electrical and Computer Engineering, Graduate University of Advanced Technology, Kerman, Iran

ABSTRACT: The escalating development of artificial intelligence and machine learning in Industry 4.0 and cyber-physical systems has heightened security challenges for humans. In addressing this, Physical Unclonable Functions (PUFs) have emerged as a promising, lightweight solution to enhance the security of Internet of Things (IoT) devices. The imperative need for secure and low-power cryptographic devices has become evident in the IoT domain and its evolving technologies. Although IoT has enabled battery-operated devices to transmit sensitive data, it has also introduced challenges, including high power consumption and security vulnerabilities. This paper presents an exploration of the utilization of adiabatic logic with Carbon Nano Tube field-effect transistors (CNTFETs) for the design of lightweight IoT devices aimed at addressing these challenges. The proposed computing platform and architecture circuit, employing Static Random-Access Memory (SRAM), demonstrate the potential to enhance security and energy efficiency for IoT applications. Our research showcases highly resilient CNTFET and adiabatic logic-based SRAM-PUFs, exhibiting an ultra-low start-up power of 1.8 nw. The PUF metrics, including uniformity, reliability, and uniqueness, are 46.10%, 88.47%, and 48.84%, respectively, across a 150% process variation. In this paper, we conduct circuit simulations using 32nm CNTFET technology in HSpice to scrutinize the impact of threshold voltage fluctuations. Further post-processing procedures are executed using MATLAB software.

Review History:

Received: Feb. 10, 2024
Revised: Jun. 03, 2024
Accepted: Jun. 30, 2024
Available Online: Jun. 30, 2024

Keywords:

Physical Unclonable Function (PUF)
Adiabatic
Carbon Nanotube Field-Effect Transistor (CNTFET)
SRAM-PUF
Low Power

1- Introduction

The Internet of Things (IoT) represents a revolutionary technological concept, aiming to create a global network connecting various devices and objects. Recognizing as a pivotal field of future technology, the IoT has captured the attention of numerous industries [1]. However, for IoT to be successful, devices must address several challenging aspects, including low energy consumption, lightweight design, and robust security measures to counter potential threats.

One promising approach for enhancing security in IoT devices is the use of Physical Unclonable Functions (PUFs), which can be likened to digital fingerprints for both silicon and non-silicon chips. PUFs offer an economical means of generating secret bits for secure systems, particularly within the context of IoT devices [2]. Despite their potential, designing a reliable and energy-efficient PUF presents a significant hurdle [2].

Silicon-based devices inherently exhibit physical variations, including internal resistance, capacitors, leakage, and oxide thickness, which pose challenges during the manufacturing process. Similarly, carbon nanotube transistors, akin to MOSFETs, possess parameters like nanotube diameter, pitch, and tox that can be altered during manufacturing, significantly impacting the threshold voltage. Various PUF topologies, such as SRAM PUF [2, 3], Arbiter PUF [4, 5], Butterfly PUF [5], Glitch PUF [6], and Ring-Oscillator (RO) [7], each have distinct advantages and disadvantages, including high power consumption and limited challenge-response pair (CRP) sets [3].

This paper investigates the application of adiabatic logic with CNTFETs in the development of lightweight IoT devices. The proposed architecture introduces a two-pronged approach to enhance PUF performance. By incorporating both adiabatic logic and advanced manufacturing techniques, the design aims to achieve superior uniformity, reliability, and uniqueness in the PUF, all while minimizing power consumption. The use of adiabatic logic minimizes energy consumption, making the architecture suitable for low-power IoT devices. Additionally, the advanced manufacturing techniques ensure that the PUF maintains high reliability and robustness, even under varying environmental conditions. The proposed computing platform and architecture utilize SRAM memory, a type of volatile memory widely found in digital devices. SRAM-PUFs, known as memory-based PUFs, take advantage of the natural variations that occur during chip manufacturing to create a unique identifier for each chip, showcasing the potential to improve security and energy efficiency for IoT applications.

*Corresponding author's email: m.monajati@kgut.ac.ir

In summary, this research aims to develop a PUF architecture that not only meets the stringent energy efficiency requirements of IoT devices but also provides enhanced security features. The proposed SRAM-PUF leverages the unique properties of CNTFETs and adiabatic logic to deliver a high-performance, low-power solution for secure IoT applications.

The rest of this article is organized as follows: Section 2 provides an overview of related work. The background of adiabatic logic and carbon nanotube transistors is elucidated in Section 3, providing a foundation for the subsequent discussions. Section 4 introduces the CNTFET SRAM-PUF cell and outlines the architecture constructed using this cell. Following that, Section 5 delves into security metrics and the power consumption analysis of the SRAM-PUF. The paper concludes in Section 6, summarizing key findings and suggesting potential avenues for future research related to the PUF.

2- Related work

Various PUF topologies have been explored, each with unique advantages and limitations. The introduction of the first adiabatic SRAM-PUF [3] in 2016 prioritized energy efficiency and precision in the context of PUF, introducing the quasi-adiabatic logic-based PUF (QUALPUF) topology, underlining the importance of hardware security in Integrated Circuits (IC) design. In this article, the widths of all the transistors are 2um and the lengths of all the transistors are 180nm, and Monte-Carlo simulation produces 200 sample devices.

In a similar vein, [2] proposed a 128-bit SRAM-based physical unclonable function (PUF) that utilizes adiabatic principles to achieve optimal characteristics in terms of uniformity, reliability, and uniqueness. The study examines two manufacturing technologies, specifically those with 45nm and 180nm nodes. Details regarding the 45nm technology are provided in our comparison table. This research addresses the need for energy-efficient and reliable 128-bit SRAM-PUFs for IoT devices, ensuring stable performance in low-power circuitry.

A quasi-adiabatic tristate PUF cell structure was suggested in 2020 [8], utilizing eight PMOS and NMOS transistors and sized with width 2um, length 180nm, and simulated at a frequency of 100 MHz. 128-bit PUF based on quasi-adiabatic tristate topology varies between 540nm and 19.8um and power exchange between 157 nw and 899 nw. In the comparison table, we have shown the least power in 2um size transistor. This design highlights the importance of secure PUFs and is directly applicable to the development of lower-power adiabatic tristate PUFs. Another significant development is a low-power, two-phase clocking adiabatic PUF that uses a trapezoidal power clock signal for improved energy efficiency and reliable start-up behavior. This design employs static CMOS 180nm logic to produce stable CRPs and controls the PUF cell's charge/discharge with a constant supply current. It demonstrates reliable performance under various conditions, including different temperatures and CMOS process variations [9]. In 2021, a CMOS Two-Phase Clocking Adiabatic PUF (TPCA-PUF) was proposed for IoT devices [10]. While the study primarily focuses on secure IoT applications, the concept of ultra-low power architectures is transferrable to IoT devices based on FinFETs. This topology incorporates an additional Vpc inverter at the top and an extra bottom transistor (controlled by the Vpc signal), enhancing the trapezoidal power clock for improved operational speed. Also in this work, the author works on both Quasi-Adiabatic logic-based PUF (QUALPUF) and the Quasi-Adiabatic logic-based PUF (TPCA-PUF) to compare two technology processes: CMOS 45nm, 180nm, and FinFETs 45nm.

Additionally, the use of advanced materials and manufacturing techniques, such as carbon nanotube field-effect transistors (CNTFETs), has been explored to improve PUF performance. CNTFET-based PUFs exhibit enhanced stability and reduced variability compared to their silicon counterparts, contributing to better uniformity, reliability, and uniqueness of the PUF responses. Research efforts in 2023 and 2024 have focused on designing SRAM-PUF circuits with carbon nanotube technology, featuring lighter topologies for improved energy efficiency in IoT devices, particularly edge devices. Additionally, the incorporation of complementary circuits further enhances the stability of these PUF circuits against unwanted noise [11, 12].

Our proposed architecture builds upon these works by integrating adiabatic logic with CNTFET technology to create a highly efficient and reliable PUF. By addressing both power consumption and environmental robustness, our design represents a significant advancement in the field of PUFs for IoT applications.

3- Background

3- 1- Adiabatic Logic

Adiabatic logic, as a clocking technique, facilitates the creation of ultra-low power circuits by efficiently recycling the charge stored in the load capacitor, thereby reducing overall power consumption. The fundamental concept underlying adiabatic logic is illustrated in Fig. 1. However, a significant limitation of adiabatic logic is its constraint to operate at frequencies lower than 1 GHz. Moreover, the use of multi-phase clocking introduces an overhead for circuits based on adiabatic logic [2].

The dissipated energy in adiabatic logic is contingent on the constant time (τ), which represents the evaluate/recover phase of the capacitor. By extending the constant time ($\tau >> RC$), adiabatic logic exhibits significantly lower energy dissipation compared to conventional CMOS logic. The expression for the dissipated energy in adiabatic logic is as follows [2]:

$$E_{adiabatic} = \frac{RC}{\tau} CV_{dd}^2 \quad (1)$$

3- 2- Carbon Nanotube Transistors

Carbon nanotube field-effect transistors (CNTFETs) emerge as a promising alternative to conventional CMOS

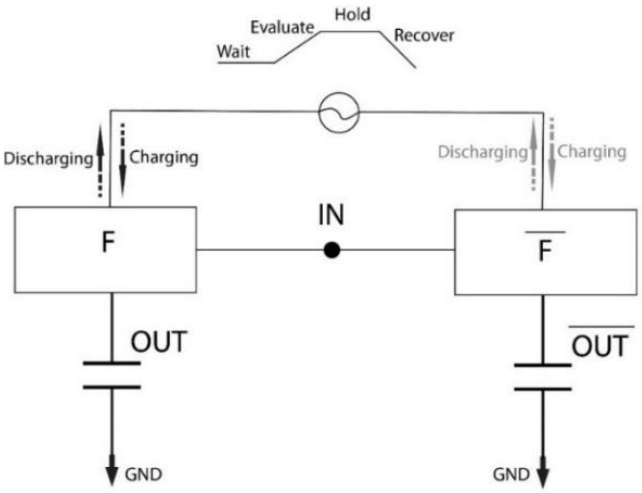

Fig. 1. Adiabatic charging/discharging technique

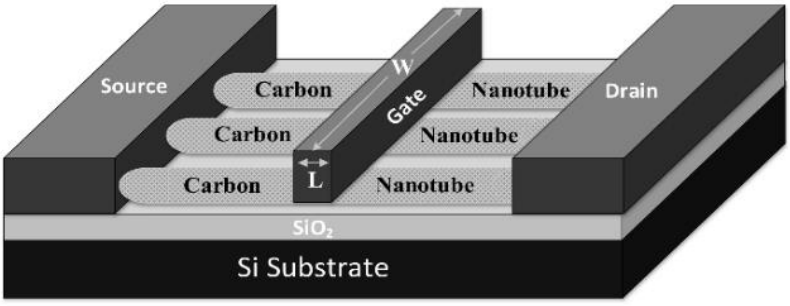

Fig. 2. Schematic of a carbon nanotube transistor (CNTFET) [13]

technology [4]. Fig. 2 depicts the structure of a CNTFET, wherein carbon nanotubes function as the channel positioned beneath the gate. These carbon nanotubes essentially consist of rolled graphene layers with specific chiral vectors dictating their electrical properties, such as conductivity or semi-conductive characteristics. CNTFETs exhibit faster operation in comparison to MOSFETs and consume lower power.

The threshold voltage of a CNTFET can be easily changed by changing the diameter of the nanotube. The following formulas are used to compute a CNTFET's threshold voltage [4]:

$$D_{cnt\,(nm)} = \frac{\sqrt{3}a_{\circ}}{\pi}\sqrt{n_1^2 + n_1 n_2 + n_2^2} = 0.0783\sqrt{n_1^2 + n_1 n_2 + n_2^2} \quad (2)$$

$$V_{th(v)} \approx \frac{E_{bg}}{2e} = \frac{\sqrt{3}}{3}\frac{aV_{\pi}}{eD_{cnt}} \approx \frac{0.43}{D_{cnt(nm)}} \quad (3)$$

Where D_{cnt} is the CNT diameter, n_1 and n_2 are the chiral vector integers, e denotes the unit electron charge, Ebg stands for the CNT bandgap, $a_{\circ}$ (approximately 0.142nm) signifies the interatomic distance between each carbon atom and its neighbor, V_{π} (approximately 3.033eV) is the carbon π-π bond energy in the tight bonding model, and a (approximately 2.49Å) is the carbon to carbon atom distance [4].

Incorporating CNTFETs in PUF circuits offers several advantages. Capitalizing on the distinctive properties of carbon nanotube transistors, these PUFs are engineered to be more secure and resilient in the face of environmental variations [4]. This renders them an appealing option for

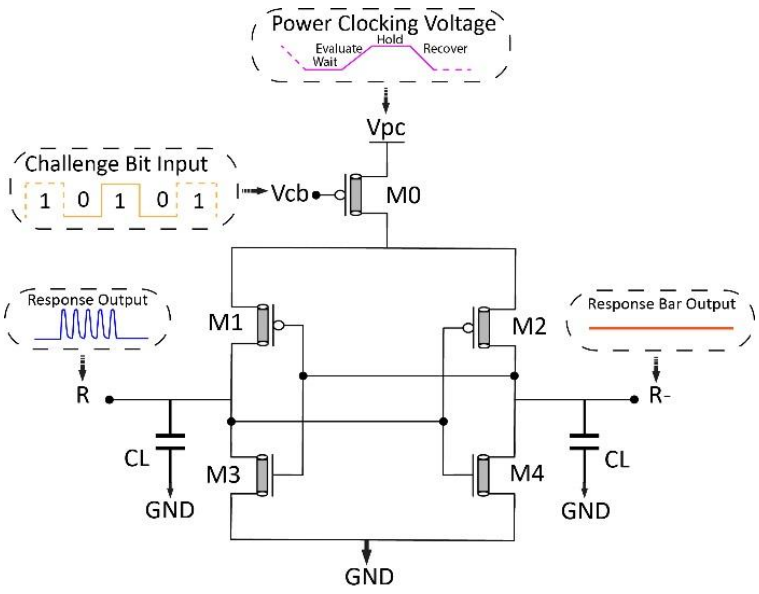

Fig. 3. Proposed SRAM-PUF cell with input and output signals

bolstering the security of IoT devices and other applications that demand robust authentication mechanisms.

4- Proposed Physical Unclonable Function Design

The proposed circuit topology of the ultra-lowpower adiabatic logic-based carbon nanotube transistor SRAM-PUF is illustrated in Fig. 3. In this configuration, Transistor M0 serves as the enable/disable PUF cell, regulating the circuit's operation. Transistors M1, M2, M3, and M4 collectively constitute the bistable structure, playing a pivotal role in generating random bits.

The generation of random bits is accomplished through process variation, stemming from differences in threshold voltage within the bistable structure. These inherent variations result in the creation of random challenge bits (Vcb). Moreover, the circuit furnishes two complementary outputs (R and R-) as integral components of its functionality. These complementary outputs play a crucial role in generating the response bits of the SRAM-PUF.

This circuit design harnesses the benefits of adiabatic logic and carbon nanotube transistors to achieve ultra-low power consumption, all the while ensuring the production of secure and random responses for PUF-based applications.

4- 1- Operation of the proposed design

The operation of the PUF cell in adiabatic logic, with four phases (wait, evaluate, hold, and recover), unfolds as follows:

Wait Phase: When the challenge bit (Vcb) is low (Vcb=0), the PUF cell activates, and transistor M0 is turned on. In this phase, the PUF cell readies itself to respond to incoming challenges.

Evaluation Phase: When the challenge bit is high (Vcb=1), the cell enters the evaluate phase of the clock, becoming inactive. During this phase, both PCNFETs (M1, M2) start conducting. Due to the variation in threshold voltage between these transistors, one of them conducts current more rapidly than the other. This discrepancy in charging times leads to complementary outputs, where one output signifies logic "1" and the other logic "0".

Hold Phase: In this phase, the PUF cell maintains a stable response. The outputs generated during the evaluation phase are preserved, ensuring the constancy and security of the PUF response.

Recovery Phase: As the clock transitions to the recovery phase, the voltage decreases from Vdd to ground, and the load capacitor discharges back to the power clock source. This readies the PUF cell for the next challenge.

The circuit's operation in adiabatic logic is visually represented in Fig. 4, illustrating the distinct phases and the behavior of the PUF cell throughout each phase. This design strives to attain ultra-low power consumption and secure PUF responses, accomplished through the strategic integration of adiabatic logic and carbon nanotube transistors.

4- 2- Design of 4-bits SRAM-PUF

Fig. 5 presents the architecture of a 4-bit cascaded SRAM-PUF, an advanced configuration that integrates multiple PUF cells in a cascading arrangement. Each individual PUF cell operates with its own dedicated power clock, precisely set with a 90-degree phase difference relative to the adjacent

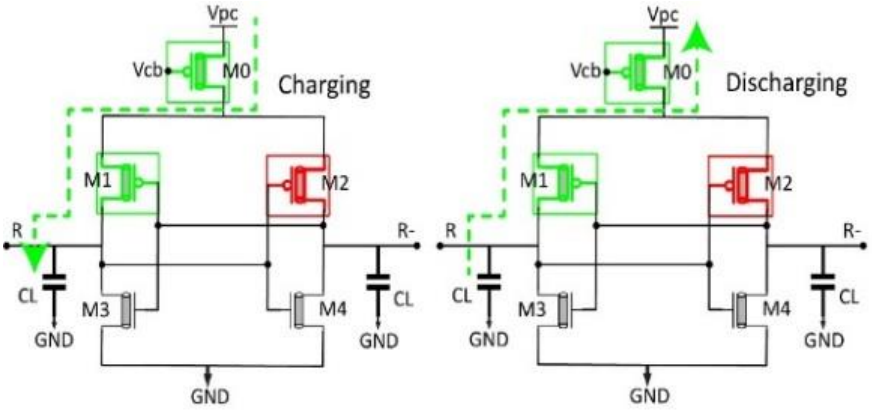

Fig. 4. Circuit operation during evaluation and recovery phases with transistor M1 featuring lower threshold voltage

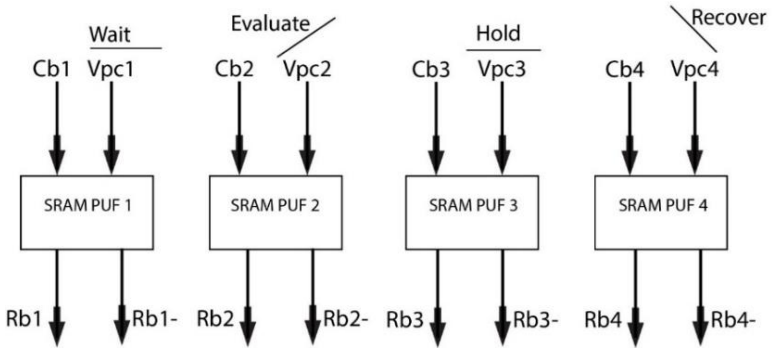

Fig. 5. 4-bit SRAM-PUF architecture

cell. This phase offset ensures accurate coordination and synchronization of the PUF cells throughout their operational cycles. The adjustment of phases is meticulously carried out using HSpice simulations to achieve the desired phase relationships, ensuring precise synchronization of the PUF cells.

For example, while the first PUF cell enters the wait phase, the subsequent cell in the same local PUF progresses to the evaluate phase. Similarly, the other two PUFs concurrently undertake their respective phases, with one in the hold phase and the other in the recovery phase [3].

This innovative cascaded design enables efficient resource utilization and maximizes the parallel processing capability of the PUF cells. By synchronizing timing and carefully shifting phases among individual PUFs, this architecture aims to optimize performance, achieve robustness, and enhance the overall security and reliability of the SRAM-PUF system.

To conserve startup power to the maximum extent, a delay is introduced in the challenge bits, equating to 1/4 of the power clock compared to adjacent bit challenges, as depicted in Fig. 6. This thoughtful addition further contributes to the system's energy efficiency and overall effectiveness.

5- Simulation results

In this study, the analysis of the 4-bit SRAM-PUF involved the utilization of the Stanford library model [14] for the baseline CNTFET with 32nm technology. The parameters of the CNTFET model and the values employed in the SRAM-PUF design are comprehensively outlined in Table 1 for reference. The simulations were conducted within the HSpice environment. Subsequent to the initial simulations, additional post-processing steps were carried out using MATLAB software. The analog output values generated by the circuit were initially extracted using HSpice and further transformed into digital values through MATLAB for in-depth analysis.

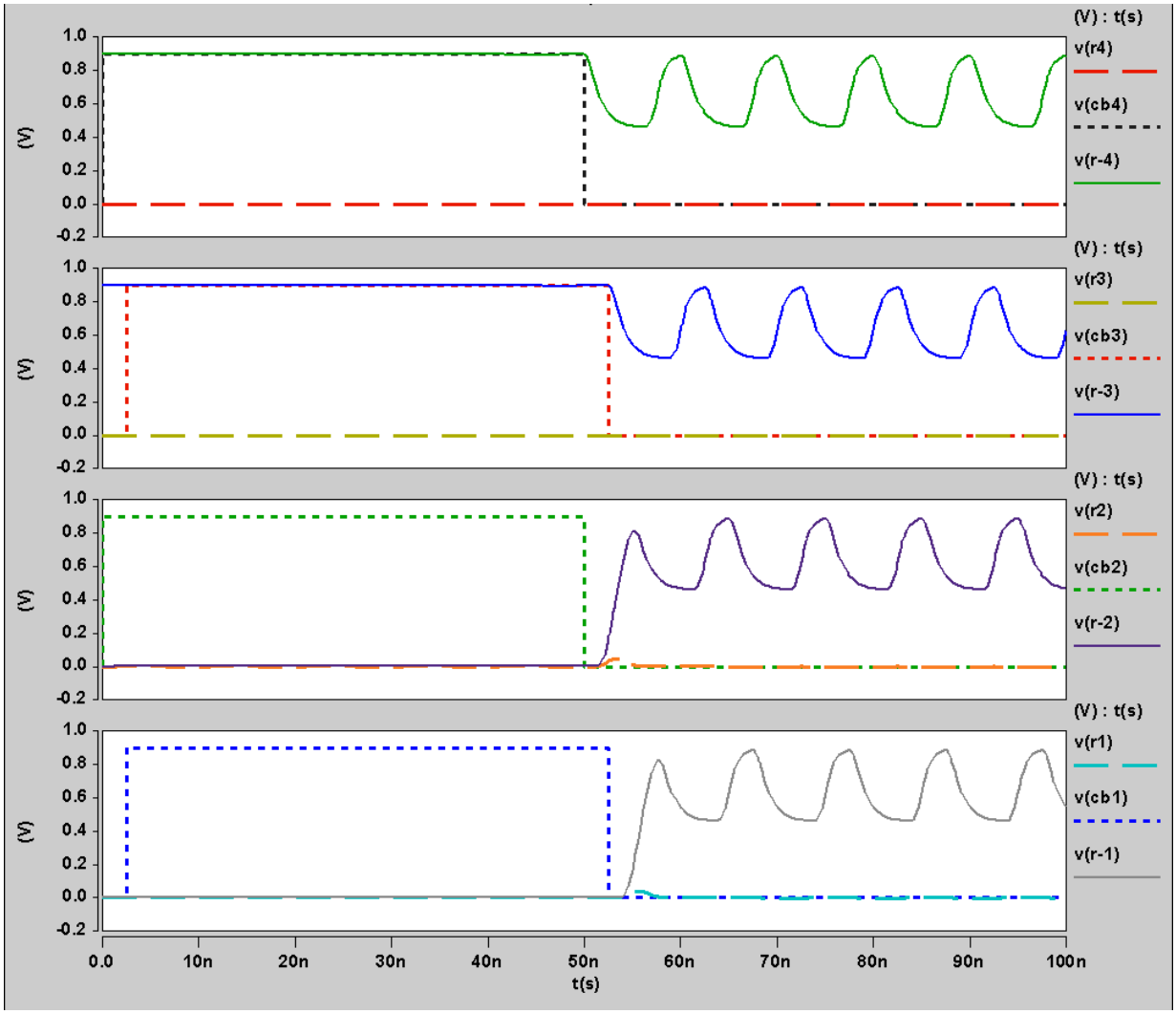

Fig. 6. Configuring the challenge bit for the minimum start-up power.

Using HSpice, a circuit simulation tool, we accurately model and simulate the behavior of the SRAM-PUF circuit, including clock signals with varying phases. Meticulously adjusting these phases within the HSpice environment allows precise control over the timing relationships among different phases, achieved by modifying delay parameters in the circuit model. This iterative optimization process fine-tunes the delay parameters until desired phase relationships are achieved, ensuring each PUF cell operates with correct timing in its respective phase (wait, evaluate, hold, or recover). Rigorous verification and validation of the adjusted phases are conducted through extensive simulation runs, analyzing waveforms and timing diagrams. Additionally, we optimize the circuit design for energy efficiency, minimizing power consumption associated with clock generation and distribution to ensure ultra-low power operation, suitable for IoT applications.

To comprehensively explore the behavior and performance of the chips under diverse conditions, we employed Monte Carlo simulations. This advanced simulation technique allowed us to replicate characteristics such as threshold voltage (with a variation of up to 150%) and temperature, providing a thorough understanding of their performance across different scenarios.

For the evaluation of PUF metrics, we adopted a meticulous approach. We manipulated the parameters that exert the most significant influence on the threshold voltage, as defined in Eq. (3). Specifically, we varied the values of *n1* and *n2*, representing the chiral vector integers in the CNTFET model. Monte Carlo simulations were conducted using HSpice software to generate output data for these PUF parameters. Subsequently, we systematically evaluated these simulation results using MATLAB software. This included calculations to assess PUF metrics, such as uniformity, reliability, and uniqueness.

This meticulous approach enabled us to thoroughly

Table 1. Parameters of the CNTFET model and corresponding values implemented in SRAM-PUF design

Parameters	Description	Value
Lch	Length of Gate/Drain/Source	32nm
Lgeff	Length of mean free path length of intrinsic CNT channel	100nm
Tox	Oxide thickness	4nm
K	Dielectric Constant	16
Pitch	distance between the centers of two adjacent CNTs	20nm
n1, n2 (M0)	Chiral vector of M0	(19,0)
n1, n2 (bistable)	Chiral vector of M1, M2, M3, M4	(10,0)
Efi	Fermi level energy of S/D Tube	0.6eV
Tubes	The number of tubes in the device	3
Csub	Coupling Capacitance	40pF/m

analyze and assess the performance of our SRAM-PUF design. By considering the effects of various parameters and environmental conditions, we achieved a comprehensive understanding of its behavior and capabilities.

The power supplies utilized in our simulations have a swing range of 0 to 0.9 V. The frequencies of the challenge bit and the power clock were set at 10 MHz and 100 MHz, respectively. Results were obtained using a reference temperature of 27°C and capacitances of 10 fF. In our simulations, we standardized the capacitance values within the SRAM-PUF cells to 10 fF as a common reference point. Although CNTFETs introduce unique characteristics that may influence overall capacitance, this standard value was chosen to maintain compatibility with industry-standard CMOS technology for SRAM cells. This choice facilitates meaningful comparisons with existing empirical data and industry benchmarks, providing a foundational assessment of the SRAM-PUF's performance. Fig. 7 illustrates the waveforms of the challenge bit, power supply, and response bit during our experiments. These waveforms offer valuable insights into the behavior of the SRAM-PUF under specific conditions.

To evaluate the performance of the SRAM-PUF, we scrutinized essential metrics including energy dissipation, uniformity, reliability, and uniqueness. These evaluation metrics furnish critical information regarding the efficiency, security, and robustness of the proposed 4-bit SRAM-PUF architecture. Through the analysis of these metrics and the execution of comprehensive simulations, our goal is to acquire deeper insights into the behavior and effectiveness of the SRAM-PUF under various scenarios. This endeavor contributes to the advancement and optimization of PUF-based security systems, particularly in the context of IoT and other applications.

Our validation approach leverages Monte Carlo simulations, renowned for capturing the statistical behavior of complex systems, effectively addressing inherent randomness and variations within our SRAM-PUF design. By systematically varying key parameters, encompassing nanotube characteristics, temperature fluctuations, and stochastic factors, we generate a diverse range of possible outcomes, closely mimicking real-world operational scenarios. Statistical analyses of the simulation data enable a robust evaluation of performance metrics, including power consumption, uniformity, reliability, and uniqueness, under varying conditions.

The alignment between Monte Carlo simulations and deterministic simulations reinforces the credibility of our results. Sensitivity and robustness analyses provide insights into the design's reliability, further strengthening the validity of our findings. Despite relying on simulations, our comprehensive approach offers a reliable basis for the presented outcomes.

5- 1- Power dissipation

The primary motivation behind the adoption of both adiabatic logic and CNTFET technology in the SRAM-PUF design is the pursuit of substantial power consumption reduction. This synergistic integration aims to mitigate energy usage, a pivotal aspect in modern electronic systems, especially for low-power applications such as IoT.

In Fig. 8, we present a comprehensive visualization of power consumption over time. This graphical representation offers a clear depiction of how the combined benefits of adiabatic logic and CNTFET technology contribute to the overarching goal of minimizing power utilization within the SRAM-PUF. By showcasing the dynamic fluctuations in power consumption throughout different operational phases,

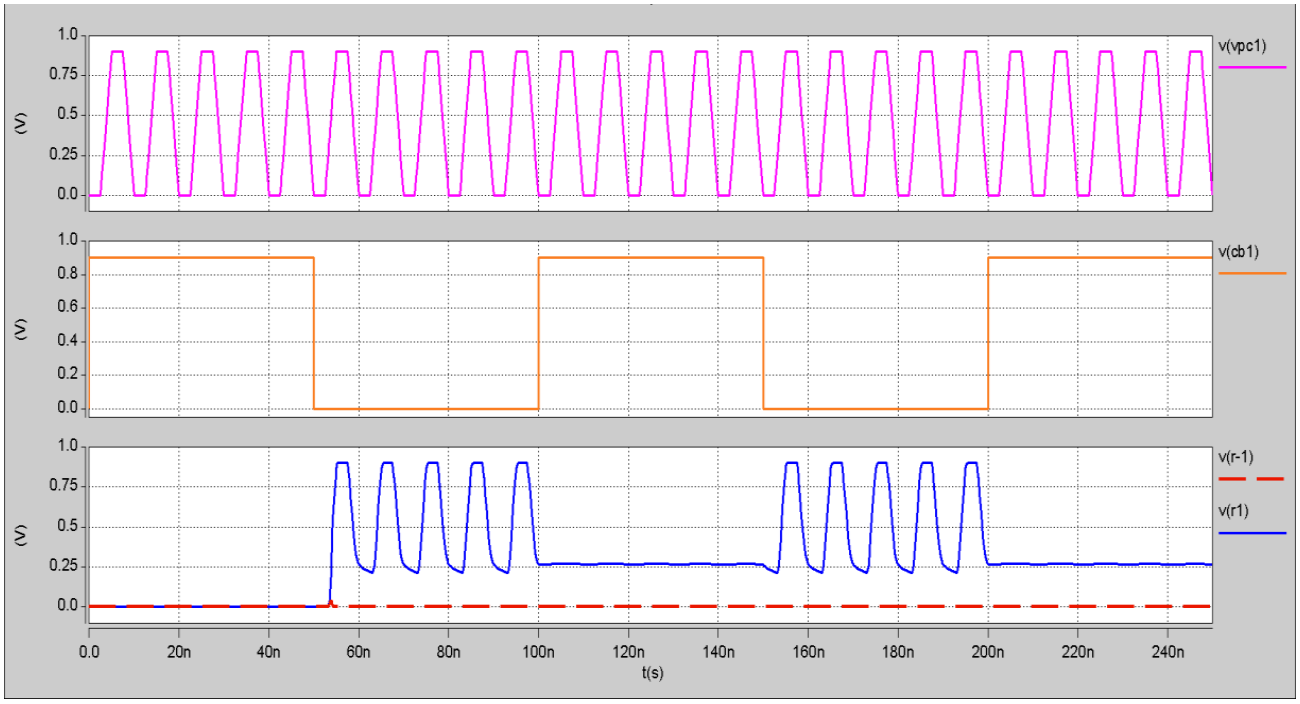

Fig. 7. Input and output signals of the SRAM-PUF cell

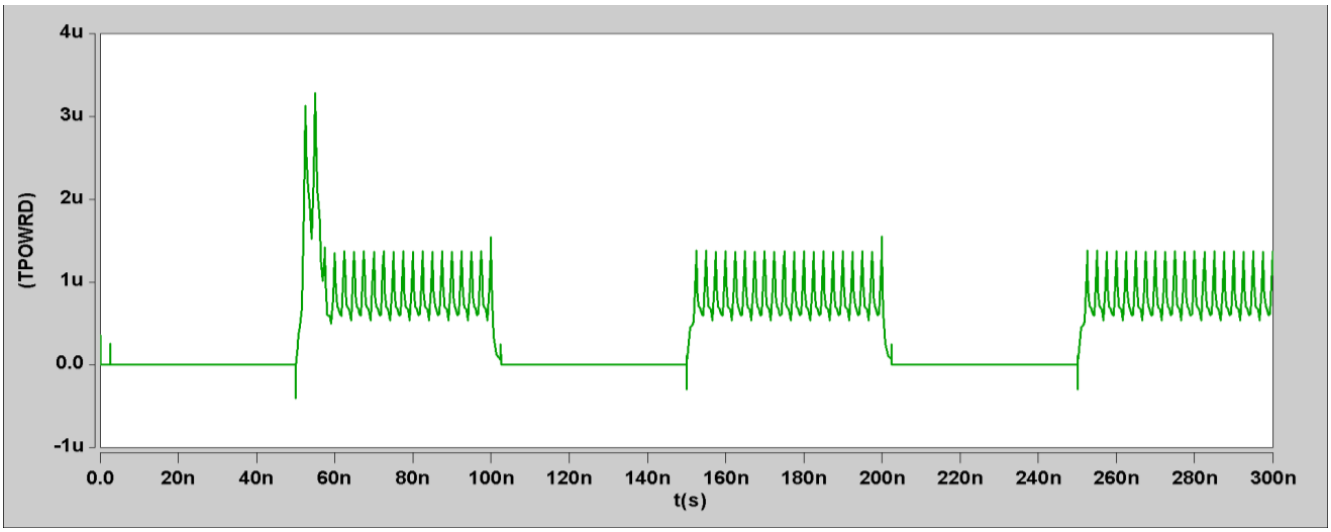

Fig. 8. Power consumption

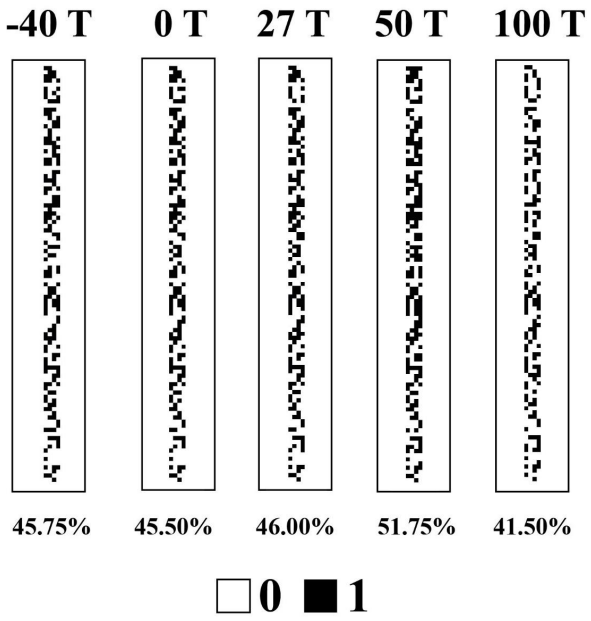

Fig. 9. Uniformity of grayscale bitmap at various temperatures

this figure substantiates the efficacy of our chosen approach in achieving enhanced energy efficiency and sustainability.

5- 2- Uniformity

Uniformity reflects the probability that the occurrence of 0s and 1s is uniformly distributed in the response bit (R). It gauges the randomness of the response bit and is calculated as the percentage of the Hamming weight (HW) of the response bit, as depicted in Eq. (4) [15].

$$Uniformity = \frac{1}{n}\sum_{l=1}^{n} r_{i,l} \times 100\% \tag{4}$$

Where *ri,l* is the *l-th* bit of the response n-bit from a chip *i*. The ideal value of uniformity is 50%. Fig. 9 shows the grayscale bit map image of the 4 × 100 SRAM-PUF.

5- 3- Reliability

The reliability of the PUF design is evaluated based on its capacity to consistently reproduce the same response bit (R) when exposed to the same challenge bit (C), even amid changing environmental conditions like supply voltage and temperature. The reliability can be quantified by computing the average intra-device hamming distance (HD) using the following Eq. (5) [15]:

$$HD_{intra} = \frac{1}{d}\sum_{t=1}^{d} \frac{HD(R_i R'_{i,t})}{n} \times 100\% \tag{5}$$

Where *Ri* represents the response of the chip *i* measured under nominal operating conditions. *R'i,t* denotes the *t-th* sample of the response *Ri*, extracted under different supply voltage and temperature conditions [15]. *n* represents the bit size of the PUF response (in this study, $n = 4$). *d* is the number of devices (chips) used in the analysis ($d = 100$ in this study), Additionally, the temperature range considered in our analysis spans from -40°C to 100°C.

$$Reliability = 100\% - HD_{intra} \tag{6}$$

5- 4- Uniqueness

The PUF's capability to differentiate a specific integrated circuit (IC) from others with the same structure using the same challenge C is quantified through its uniqueness. When two chips, *i* and *j* (where $i \neq j$), receive the same challenge C, and their responses are denoted as *Ri* and *Rj*, the average inter-device uniqueness can be expressed as follows [15]:

$$Uniqueness = \frac{2}{d(d+1)}\sum_{i=1}^{d-1}\sum_{j=i+1}^{d} \frac{HD(R_i R_j)}{n} \times 100\% \tag{7}$$

Where *d* represents the number of devices (ICs) being compared, *n* denotes the bit length of the PUF responses. *HD* (*Ri Rj*) signifies the hamming distance between the responses of the two distinct PUFs (*Ri* and *Rj*) [15].

The optimal value for uniqueness is 50%, signifying

that each PUF response is entirely distinct from the others, leading to perfect discrimination capability among individual ICs. A higher uniqueness percentage indicates the stronger ability of the PUF to differentiate between different devices, enhancing its effectiveness and security in applications such as authentication and anti-counterfeiting measures.

The computed uniformity, reliability, and uniqueness results, based on Eqs. (4), (6), and (7), respectively, are visually depicted in Figs. 10, 11, and 12. These figures illustrate the variations in uniformity, reliability, and uniqueness under threshold voltage and temperature variations, respectively. The study employs a bit size of n = 4 and a total of 100 devices (d = 100) for the analysis.

We minimize the power consumption of our SRAM-PUF design by adjusting the values of *n1*, *n2*, and the number of *tubes* in devices, where *n1* and *n2* represent the chiral vector integers in the CNTFET model. Additionally, the implementation of a delayed challenge bit significantly contributes to reducing start-up power consumption. This approach strategically defers the activation of certain circuit elements within the SRAM-PUF design until a later stage in the authentication process. By postponing the energization of these components, we mitigate the initial surge in power typically observed during start-up, thereby enhancing energy efficiency. Through the analysis of uniformity, reliability, and uniqueness metrics, this study aims to assess and validate the robustness and security of the proposed PUF design in real-world scenarios, considering the impact of environmental

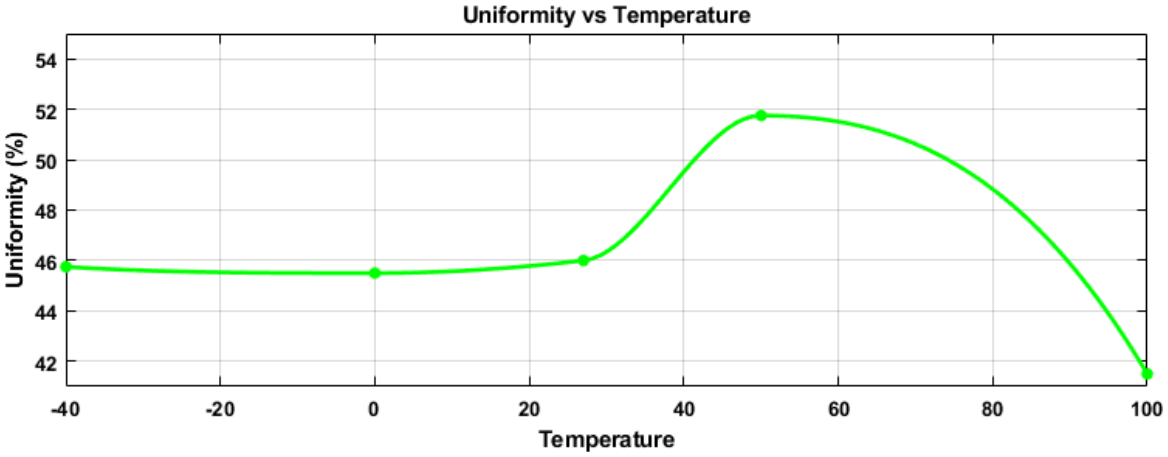

Fig. 10. Uniformity of the SRAM-PUF under the threshold voltage variation

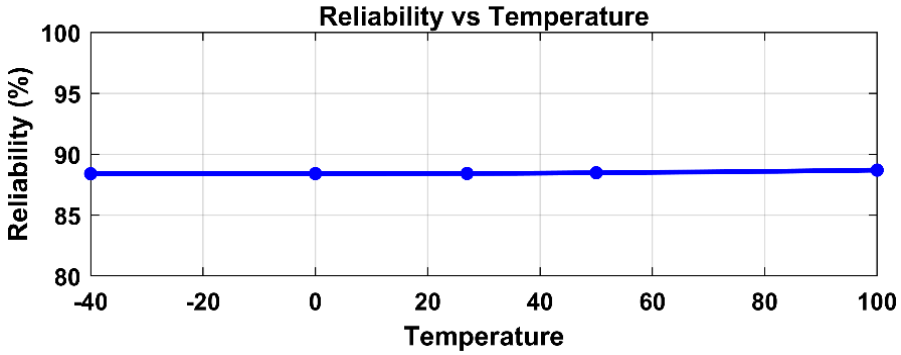

Fig. 11. Reliability of the SRAM-PUF under the threshold voltage variation

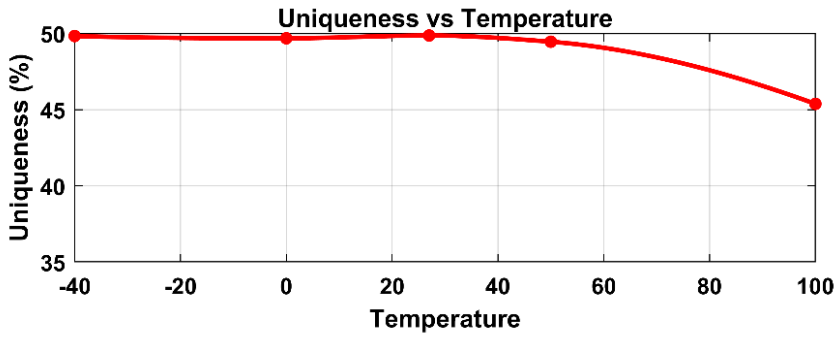

Fig. 12. Uniqueness of the SRAM-PUF under the threshold voltage variation

Table 2. Comparative analysis of PUF parameters in various designs

PUF	[3]	[2]	[8]	[10]	[10]	This work
Tech-Process (nm)	CMOS-180	CMOS-45	CMOS-180	FinFET-45	FinFET-45	CNTFET-32
Topology	Quasi-Adiabatic	Quasi-Adiabatic	Quasi-Adiabatic Tristate	Quasi-Adiabatic	Two-Phase Clocking	Quasi-Adiabatic
Bit-length	128	128	128	4	4	4
Transistor counts	5	5	8	5	7	5
Start-up power (nw)	3080	9840	157.5	65.69	18.32	1.8
Uniformity (%)	52.343	49.41	44.53	NA	NA	46.10
Reliability (%)	96.20	99.60	99.82	99.47	99.57	88.47
Uniqueness (%)	40.50	49.48	50.27	49.46	50.13	48.84

variations on its performance. In Table 2, we present a comparative analysis of various PUFs reported in the literature alongside our work. In the table, "NA" denotes data that is not available. The paper [10] provided a simulation of a PUF circuit in two distinct forms of adiabatic topology (quasi-adiabatic and two-phase Clocking), and both findings are shown in Table 2. We evaluate the key characteristics and performance metrics of each PUF design to highlight the strengths and advantages of our proposed approach. This comparison offers valuable insights into the uniformity, reliability, uniqueness, and energy efficiency of different PUF designs, showcasing the superiority and effectiveness of our ultra-low power SRAM-PUF based on CNTFETs for IoT devices.

6- Conclusion

This paper presents an innovative adiabatic logic-based approach to design an efficient SRAM-PUF using only five carbon nanotube transistors. The simulation results showcase a successful implementation with promising performance. In comparison to leading PUFs, our design achieves substantial reductions in start-up power consumption, positioning it as a compelling choice for energy-efficient IoT devices. Despite a reduction in reliability attributed to a 150% increase in process variation compared to the 10% observed in comparable references, it is noteworthy that reduced process variation is associated with increased reliability in semiconductor devices.

Numerical comparisons reveal a noteworthy reduction of

approximately 97.26% in start-up power when compared to the quasi-adiabatic [10], and a significant 90.19% reduction compared to the two-phase clocking PUF [10]. Additionally, there is an impressive nearly 98.85% reduction compared to PUF [8] and an outstanding 99.94% reduction compared to PUF [3]. These substantial advancements in power efficiency underscore the superiority of our ultra-low power SRAM-PUF based on CNTFETs, positioning it as an excellent choice for energy-efficient IoT devices. Despite the observed reduction in reliability, our proposed design exhibits compelling advantages in power optimization, making it a promising and competitive option for IoT applications.

We underscore the potential of carbon nanotube transistors for future PUF advancements and recommend exploring ferroelectric CNTFET technology for even greater power optimization and performance gains [16]. In summary, this work contributes valuable insights and lays the foundation for the development of more efficient and secure VLSI circuits, particularly in the context of IoT applications. The innovative use of adiabatic logic with CNTFETs holds promise for addressing the energy efficiency challenges in IoT devices, paving the way for future advancements in semiconductor technology.

References

[1] I. Lee, K. Lee, The Internet of Things (IoT): Applications, investments, and challenges for enterprises, Business horizons, 58(4) (2015) 431-440.

[2] S.D. Kumar, H. Thapliyal, Design of adiabatic logic-based energy-efficient and reliable PUF for IoT devices, ACM Journal on Emerging Technologies in Computing Systems (JETC), 16(3) (2020) 1-18.

[3] S.D. Kumar, H. Thapliyal, Qualpuf: A novel quasi-adiabatic logic based physical unclonable function, in: Proceedings of the 11th Annual Cyber and Information Security Research Conference, 2016, pp. 1-4.

[4] H. Momeni, A. Ghazizadeh, F. Sharifi, Multi-valued logic arbiter PUF designs based on CNTFETs, Computers and Electrical Engineering, 102 (2022) 108295.

[5] K. Devika, R. Bhakthavatchalu, FPGA implementation of programmable Hybrid PUF using Butterfly and Arbiter PUF concepts, in: Journal of Physics: Conference Series, IOP Publishing, 2022, pp. 012033.

[6] D. Suzuki, K. Shimizu, The glitch PUF: A new delay-PUF architecture exploiting glitch shapes, in: International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2010, pp. 366-382.

[7] A.A. Zayed, H.H. Issa, K.A. Shehata, FinFET based low power ring oscillator physical unclonable functions, in: 2019 31st International Conference on Microelectronics (ICM), IEEE, 2019, pp. 227-230.

[8] S. Hemavathy, V.K. Bhaaskaran, Design and analysis of secure quasi-adiabatic tristate physical unclonable function, in: 2020 IEEE International symposium on smart electronic systems (iSES)(Formerly iNiS), IEEE, 2020, pp. 109-114.

[9] C. Monteiro, Y. Takahashi, Low-power two-phase clocking adiabatic PUF circuit, Electronics, 10(11) (2021) 1258.

[10] C. Monteiro, Y. Takahashi, Ultra-low-power finfets-based tpca-puf circuit for secure iot devices, Sensors, 21(24) (2021) 8302.

[11] A. Shafiei, M. Monajati, Ultra-Low Power SRAM-PUF for IoT Devices Based on CNTFETs, in: 2023 5th Iranian International Conference on Microelectronics (IICM), IEEE, 2023, pp. 86-90.

[12] A. Shafiei, M. Monajati, Lightweight SRAM-PUF Identity Authentication for Edge Devices, in: 2024 32nd International Conference on Electrical Engineering (ICEE), IEEE, Tehran, Iran, 2024, pp. 1-5.

[13] F. Zahoor, F.A. Hussin, F.A. Khanday, M.R. Ahmad, I. Mohd Nawi, C.Y. Ooi, F.Z. Rokhani, Carbon nanotube field effect transistor (cntfet) and resistive random access memory (rram) based ternary combinational logic circuits, Electronics, 10(1) (2021) 79.

[14] Stanford, Stanford University CNFETModel (Available:http://nano.stanford.edu/model.php?id=23.), in, 2008.

[15] A. Al-Meer, S. Al-Kuwari, Physical unclonable functions (PUF) for IoT devices, ACM Computing Surveys, 55(14s) (2023) 1-31.

[16] M.K.Q. Jooq, M.H. Moaiyeri, K. Tamersit, A new design paradigm for auto-nonvolatile ternary SRAMs using ferroelectric CNTFETs: From device to array architecture, IEEE Transactions on Electron Devices, 69(11) (2022) 6113-6120.

HOW TO CITE THIS ARTICLE

A. R. Shafiei, M. Monajati. Efficient and Lightweight IoT Security Using CNTFET-Based Ultra-Low Power SRAM-PUF. AUT J. Elec. Eng., 57(1) (2025) 31-42.

DOI: 10.22060/eej.2024.22989.5578