Design of an SLIM Cipher S-box with 8T-SRAM CiM for Energy-Efficient, Lightweight, and DPA Resistant Edge AI

Koteswararao Penumalli
Department of Electronics and Communication Engineering, School of Engineering and Applied Sciences, SRM University, Amaravati, Guntur 522502, Andhra Pradesh, India
koteswara_p@srmap.edu.in

Tirumala Rao Kadiyam
Department of Electronics and Communication Engineering, School of Engineering and Applied Sciences, SRM University, Amaravati, Guntur 522502, Andhra Pradesh, India
tirumalarao_k@srmap.edu.in

Venu Birudu
Global Foundries, Bengaluru, Karnataka, India
venu.birudu@globalfoundries.com

Venkateswarlu Gonuguntla
Symbiosis Centre for Medical Image Analysis, Symbiosis International (Deemed University), Pune 412115, India
venkateswarlu.phd@gmail.com (corresponding author)

Ramesh Vaddi
Department of Electronics and Communication, School of Engineering and Applied Sciences, SRM University, Amaravati, Guntur 522502, Andhra Pradesh, India
ramesh.v@srmap.edu.in (corresponding author)

Received: 2 May 2025 | Revised: 4 June 2025 and 18 June 2025 | Accepted: 21 June 2025

 DOI: https://doi.org/10.48084/etasr.11870

ABSTRACT

Side-channel attacks pose a significant threat to the security and trustworthiness of edge Artificial Intelligence (AI) devices, especially with the rise of AI-based hardware applications. In this work, a lightweight 8T-SRAM Computing-in-Memory (CiM) SLIM cipher S-box is proposed, with enhanced energy efficiency and resiliency to Differential Power Analysis (DPA) attacks. For the first time, the design utilizes Negative Capacitance Field-Effect Transistors (NCFETs). The reconfigurable nature of the proposed CiM architecture, in conjunction with the unique steep slope characteristics of NCFET-based logic gates, contributes to the enhancement of the overall S-box design's DPA resiliency and energy efficiency. The simulation results indicate that the proposed NCFET-based 8T-SRAM CiM S-box for the SLIM cipher exhibits ~3.8× lower energy consumption in comparison with the non-CiM S-box design at V_{DD}=0.5 V. The security evaluation of the proposed NCFET-based 8T-SRAM CiM S-box design for DPA attack demonstrates a 32× increase in the attacker effect ratio, a ~2.2× reduction in Signal-to-Noise Ratio (SNR), a ~43.4× improvement in the Security Power Delay (SPD), and a 32× increase in Measurements to Disclosure (MTD). These findings signify the enhanced security and trustworthiness of the 8T-SRAM CiM-based S-box design for SLIM cipher used in edge AI devices.

Keywords-Computing-in-Memory (CiM); Differential Power Analysis (DPA) attack; hardware security; SRAM; trustworthy AI edge devices; ultra-lightweight block ciphers

I. INTRODUCTION

As Artificial Intelligence (AI) is increasingly implemented in Internet of Things (IoT) edge devices, there is a significant demand for secure and trustworthy edge AI devices for fair, unbiased, privacy-preserving, and explainable AI applications [1]. Offshore production of Integrated Circuits (ICs) increases the vulnerability of hardware to various security attacks due to potential unauthorized access, information leakage, and the risk of hardware Trojan insertion, etc., during manufacturing processes [2]. According to the National Institute of Standards and Technology (NIST), there has been a significant increase in hardware security vulnerabilities over the past few years [3]. Furthermore, the market for hardware security primitives or systems is experiencing rapid growth to prevent hardware reverse engineering, IC counterfeiting, and Side-Channel Analysis (SCA) [4]. Of the various types of hardware security attacks, SCA has proven to be highly successful in retrieving concealed sensitive information [5]. The SCA approach leverages side-channel signals, including power consumption, electromagnetic fields, and photonic emissions to uncover the encryption key of cryptographic circuits and systems [6-8]. The Differential Power Analysis (DPA) attack involves analyzing the power consumption of the encryption engine to recover secret key information with minimal effort compared to other methods [9]. The static CMOS logic style in circuit design is more susceptible to DPA attacks because of its data-dependent power consumption profile [10, 11].

To address DPA attacks, a variety of DPA countermeasures specific to CMOS-based systems have been proposed at various levels of abstraction, including device, circuit, and design considerations [12, 13]. Researchers are currently also exploring post-CMOS device technologies, such as Carbon Nanotube FET (CNTFET), Tunneling FET (TFET), Negative Capacitance FET (NCFET), and Spin-Transfer Torque Magnetic Random Access Memory (STTMRAM) devices, due to their potential for energy-efficient and secure circuit designs [14-20]. Spin-Transfer Torque Magnetic Random Access Memory (STT-MRAM) is an emerging non-volatile memory technology that stores data by manipulating the magnetic orientation of ferromagnetic layers instead of using electric charge. Among the potential emerging devices for secure and energy-efficient devices, NCFETs have proven edge over others because of CMOS compatibility and enhanced performance [17-21]. In [21], authors propose an NCFET-based PRESENT-80 cipher design and have done a preliminary analysis to explore NCFET suitability for DPA resilient cipher designs. The static CMOS SCA countermeasures are more susceptible to DPA attacks due to the high data-dependent power consumption profiles and are not energy efficient [10, 11]. To address this concern, researchers have recently explored Computing-in-Memory (CiM) architectures for improved energy efficiency and increased DPA resiliency [22]. The XOR-CiM architecture in this paper enhances hardware security by implementing XOR encryption with minimal overhead and improving ~1.4× energy efficiency without throughput loss [22].

Authors in [23] introduce an XOR-based Feistel cipher in SRAM array for in-memory encryption with ~96.14% delay reduction compared to conventional methods. A multicore SRAM CiM-based accelerator with a lightweight network for sparse convolutional neural network computing has been presented in [24], achieving high energy efficiency and performance on the CIFAR10 dataset. In [25], an 8T-SRAM-CiM macro for full-array Boolean logic and copy operations has been demonstrated with an energy efficiency of 63% compared to von Neumann architecture with application to lightweight block ciphers. Further in [26], authors discuss SRAM-based CiM for data-centric applications with the potential for lightweight block ciphers.

Supporting XNOR operations and binary convolution calculations has been demonstrated for the high energy efficiency of lightweight block ciphers [27]. An 8T-SRAM-based CiM accelerator macro with high throughput and energy efficiency suitable for lightweight block ciphers has been presented in [28]. Authors in [29] propose a SRAM-based CiM architecture for high-precision MAC operations in edge-AI devices, enhancing energy efficiency and reducing data movement. In [30], authors proposed an NCFET-based SRAM CiM technique for Deep Neural Network (DNN) applications with ~11.9 times lower energy consumption compared to CMOS CiM designs. To the best of our knowledge, not many have explored the NCFET 8T-SRAM CiM design for S-box DPA resiliency and energy efficiency for enhancing security and trustworthiness of edge AI devices. As the NCFET can offer higher noise margins and lower energy consumption compared to existing CMOS technology, it will enhance the productivity of CiM architectures and the overall S-box design's DPA resiliency. [19, 30].

The major contributions of the paper are as follows:

1. Design and analysis of NCFET-based 8T-SRAM CiM cell and CiM logic gates for use in ultra-lightweight SLIM cipher S-box.
2. Design and implementation of a lightweight 8T-SRAM CiM SLIM cipher S-box with enhanced energy efficiency, exploring NCFETs.
3. Hardware security evaluation of the proposed 8T-SRAM CiM-based S-box design for DPA attack resiliency and performance benchmarking with existing CiM and non-CiM designs.

II. NCFET DEVICE STRUCTURE AND CHARACTERISTICS WITH PROPOSED 8T-SRAM CELL DESIGN AND ANALYSIS

A. NCFET Device Structure and Characteristics

The NCFET device structure utilizes a Ferro-Electric (FE) material within the transistor's gate stack to produce a negative capacitance effect, as illustrated in Figure 1. The incorporation of the FE layer induces an internal voltage amplification, resulting in higher charge density within the transistor channel, thereby leading to an increase in device ON-current (I_{ON}) [31]. The internal voltage amplification A_V is shown in (1), derived from the capacitor equivalent model of NCFET [29].

$$A_V = \frac{|C_{fe}|}{|C_{fe}|-|C_{int}|} \quad (1)$$

where C_{fe} is the FE capacitance and C_{int} is the internal capacitance.

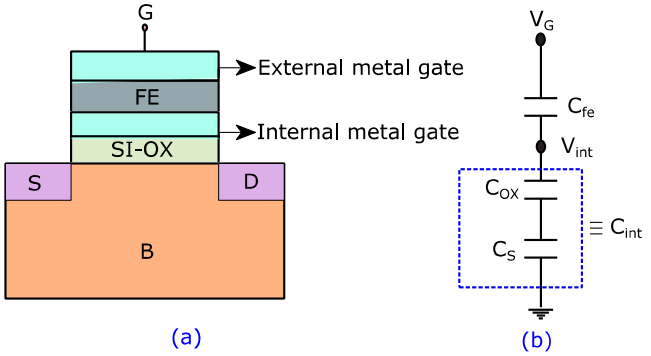

Fig. 1. (a) NCFET structure,and (b) capacitor equivalent circuit.

The FE capacitance (C_{fe}) is defined as the ratio between gate charge density (Q) and potential drop across C_{fe}, and is inversely proportional to T_{fe}, as shown in (2) [31].

$$C_{fe} = \frac{\partial Q}{\partial V_{fe}} = \frac{1}{T_{fe(2\alpha+12\beta Q^2+30\gamma Q^4)}} \quad (2)$$

As T_{fe} decreases, the magnitude of $|C_{fe}|$ increases, leading to a steeper slope. Conversely, as T_{fe} increases, the slope gradually decreases according to (2) and $|C_{fe}|$approaches C_{int}, resulting in an increase in A_V (or V_{int}) and a reduction in the subthreshold swing (SS_{NCFET}), as detailed in (3) [32].

$$SS_{NCFET} = 60\left(1 + \frac{C_{dep}}{C_{ox}}\right) \frac{|C_{fe}|}{|C_{fe}| - |C_{int}|} \quad (3)$$

where C_{ox} signifies the gate oxide capacitance and C_{dep} represents the capacitance of the depletion layer.

The behaviour of the FE oxide layer in creating a NCFET model is described using the Landau-Khalatnikov (L-K) equation [31]. Baseline 40 nm silicon MOSFETs of both p-type and n-type are incorporated in the designs, and the MIT Virtual Source Ferroelectric (MVSNC) model is employed to effectively capture the unique characteristics of NCFETs [31]. Table I presents the NCFET device parameters [31]. The $I_D - V_{GS}$ characteristics of the n-channel NCFET device for varying T_{fe} values are illustrated in Figure 2. The results indicate that, at a T_{fe} of 5 nm, the NCFET exhibits superior ON current and improved performance over the baseline CMOS, particularly at an operating voltage of 0.5 V.

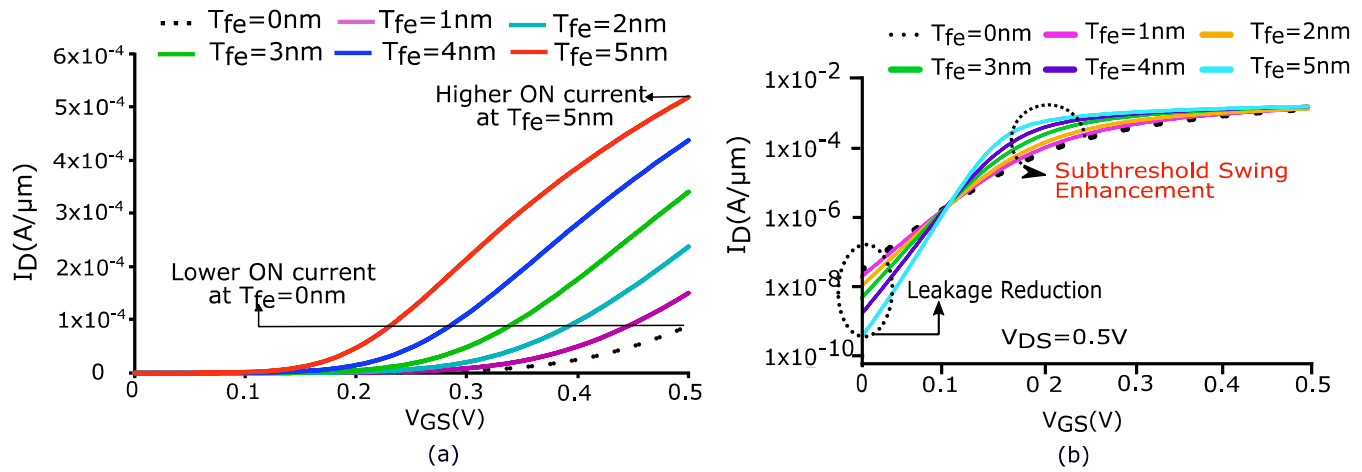

Fig. 2. (a) $I_D - V_{GS}$characteristics fordifferent FE layer thicknesses (T_{fe}), (b) log scale$I_D - V_{GS}$characteristics highlighting subthreshold behavior for varyingT_{fe} values.

TABLE I. NCFET DEVICE PARAMETERS

Symbol	Device parameter	Value
W	Transistor width	1.0e-06 cm
L_{gdr}	Length of the gate	4.0e-06 cm
E_c	Coercive field	6.5e+09 V/cm
T_{fe}	Thickness of FE layer	5.0e-11 cm
P_o	Remnant polarization	2.5e+02 C/cm^2
dL_g	Overlap length including both source and drain sides	7.56e-7 cm

B. NCFET 8T-SRAM Cell Design and Read/Write Operations

The proposed NCFET-based 8T-SRAM bit-cell design is shown in Figure 3(a). It is comprised of two distinct subcircuits. The upper subcircuit features a 6T-SRAM cell with two cross-coupled inverters and two write-access transistors (T5 and T6), which are governed by a word line (WL) signal. The lower sub-circuit consists of bit line access transistors (T7 and T8) that are controlled by a dedicated read word line signal (RWL).

To initiate a write operation, the write port is activated by enabling WL and setting the write bit lines (WBL and WBLB) to their respective voltage levels. To store a data bit of '0' in a cell, the WBL and WBLB signals are configured to '0' and V_{DD}, respectively. Conversely, the signals are set to V_{DD} and '0', respectively, to store a data bit of '1' in the cell, as illustrated in Figure 3(b).

The read operation of the 8T-SRAM-based on NCFET is also demonstrated in Figure 3(b). The read bit lines (RBL and

RBLB) are initially pre-charged and subsequently left floating. To read data from a memory cell, a negative pulse is applied to the RWL, causing either RBL or RBLB to discharge depending on the stored data in the cell. When the cell contains the data bit '0', it causes the corresponding storage nodes to have values Q=0 and Q_b=1. As a result, the complementary RBLB is discharged by T8. Similarly, when the cell contains the data bit '1', the values of the corresponding storage nodes become Q=1 and Q_b=0. This causes the RBL to be discharged through T7.

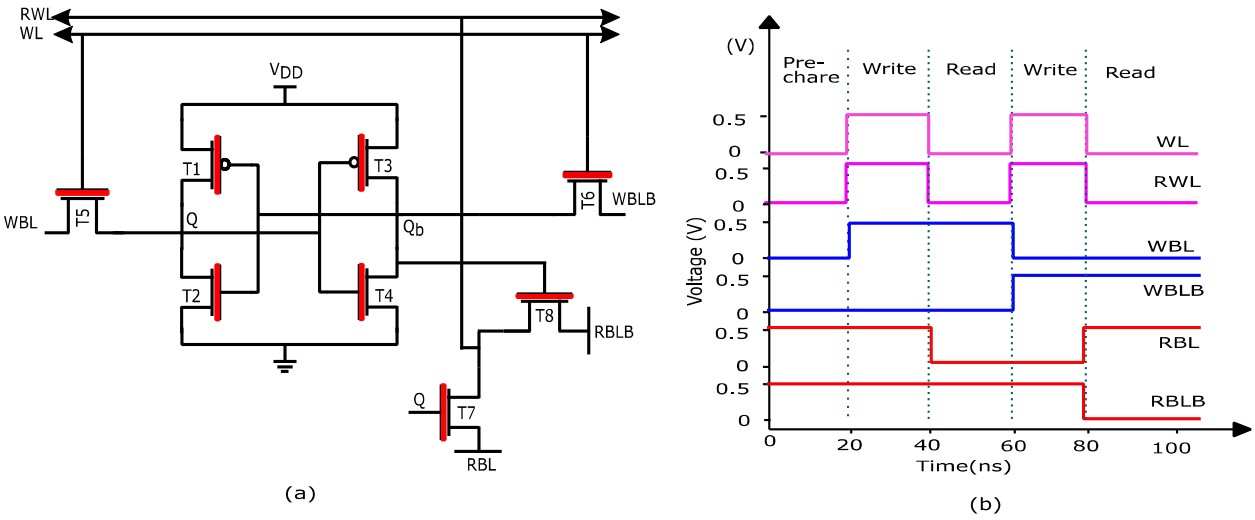

Fig. 3. (a) Schematic of the proposed NCFET-based 8T-SRAM cell design, and (b) read and write operation waveforms of the NCFET-based 8T-SRAM cell.

C. Perfromance Analysis of NCFET-based 8T-SRAM Cell Design with Varying Ferroelectric Layer Thickness

In this performance analysis, two key metrics are examined: read stability, assessed through the Read Noise Margin (RNM), and write ability, evaluated through the Write Noise Margin (WNM).

1) Write Ability

The write ability has been assessed by measuring the write noise margin, achieved by sweeping the storage nodes (Q, Q_b) of the memory cell. The NCFET-based SRAM cell demonstrates a larger square in the butterfly curves observed from the voltage transfer characteristics (VTCs) of the 8T-SRAM cell, in comparison to the baseline 8T-SRAM design. Increasing the T_{fe} from 1 nm to 5 nm results in a ~11.77% improvement in WNM at a V_{DD} of 0.5 V for an optimal T_{fe} of 3 nm. Table II summarizes the power, delay, and energy consumption of the NCFET-based 8T-SRAM cell for varying T_{fe} during write operation. For an optimal T_{fe} value of 3 nm, the NCFET-based 8T-SRAM cell design consumes ~1.42 times less energy compared to the baseline 8T-SRAM cell design during a write operation.

TABLE II. PERFORMANCE ANALYSIS OF NCFET-BASED 8T-SRAM CELL WITH VARYING FE LAYER THICKNESS DURING WRITE MODE

T_{fe} (nm)	Power (nW)	Delay (ps)	Energy (aJ)
0	30.5	19.23	1.17
1	33.7	15.41	1.04
2	35.4	12.58	0.89
3	42.1	9.80	0.82
4	52.0	8.12	0.84
5	61.6	7.12	0.87

2) Read Stability

The read stability of the 8T-SRAM cell is determined through RNM analysis during read operations. RNM is calculated based on the butterfly curves derived from the VTCs of the two cross-coupled inverters within the SRAM cell. Higher RNM values are observed with NCFET 8T-SRAM cell at an optimal T_{fe} value due to the steep subthreshold slope characteristic of the device. At a T_{fe} of 3 nm, the read Static Noise Margin (SNM) is ~18.2% higher compared to the baseline 8T-SRAM cell design at a V_{DD} of 0.5 V.

As illustrated in Table III, the read energy consumption of an NCFET 8T-SRAM cell with a T_{fe} of 3 nm is ~1.6 times lower at a V_{DD} of 0.5 V compared to that of the baseline 8T-SRAM cell. To improve the stability and energy efficiency of NCFET-based designs, it is recommended to keep T_{fe} within the range of 1–3 nm.

TABLE III. PERFORMANCE ANALYSIS OF NCFET-BASED 8T-SRAM CELL WITH VARYING FE LAYER THICKNESS DURING READ MODE

T_{fe} (nm)	Power (µW)	Delay (ps)	Energy (fJ)
0	0.21	3125.5	1.31
1	0.49	1148.2	1.12
2	1.58	242.8	0.87
3	4.9	83.64	0.82
4	12.5	43.8	1.09
5	29.8	18.9	1.13

III. PROPOSED ENERGY EFFICIENT NCFET-BASED 8T-SRAM CIM LOGIC GATES FOR LIGHTWEIGHT CIPHER DESIGN

CiM logic gates combine memory and computation operations within a single structure, making difficult for attackers to perform DPA attacks. This method also offers significant benefits in decreasing energy consumption and latency in computations when compared with Von-Neumann architectures.

A. NCFET-based 8T-SRAM Computing-in-MemoryOR Logic Design

The NCFET CiM OR logic design based on the NCFET 8T-SRAM cell is shown in Figure 4(a). The design functions in two distinct modes: memory mode and computing mode. In memory mode, the information stored in the memory cell is accessed during the write operation. The write operation of the CiM OR using NCFET is illustrated in Figure 4(b). As shown in Figure 4(b), when the WL is high during memory mode, the WBL stores its value in the memory cell, which is represented as input A. To conduct in-memory calculations within the cell, the data stored (Q) during memory mode serve as the first input A, whereas the RWL is regarded as the second input B. For the CiM OR operation, if either input A or B is '1', the output is '1'. If both inputs A and B are '0', the output will be '0', as shown in Figure 4(b).

B. NCFET-based 8T-SRAM Computing-in-Memory XOR Logic Design

The NCFET CiM XOR logic design is presented in Figure 5(a). During the write operation, the write port is activated by enabling the WL and setting WBL/WBLB to the appropriate voltage levels, as illustrated in Figure 5(b). From Figure 5(b), in memory mode, when WL is high, the WBL value is stored in the memory cell, which represents the input A. Performing in-memory computations within the cell involves using the stored data (Q/Q_b) as the input A and the RWL as the second input B. When carrying out the CiM XOR operation, the result will be '0' when inputs A and B are identical, either '0' or '1'. If the inputs are different, the output will be '1', as illustrated in Figure 5(b).

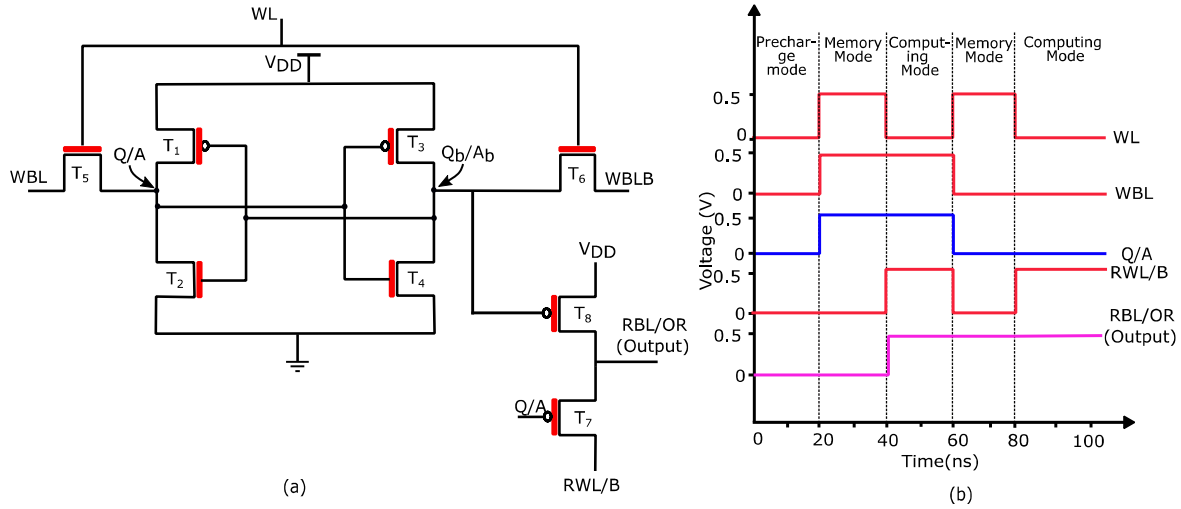

Fig. 4. (a) NCFET-based 8T-SRAM CiM OR logic design,and (b) transient response characteristics of the 8T-SRAM CiM OR logic.

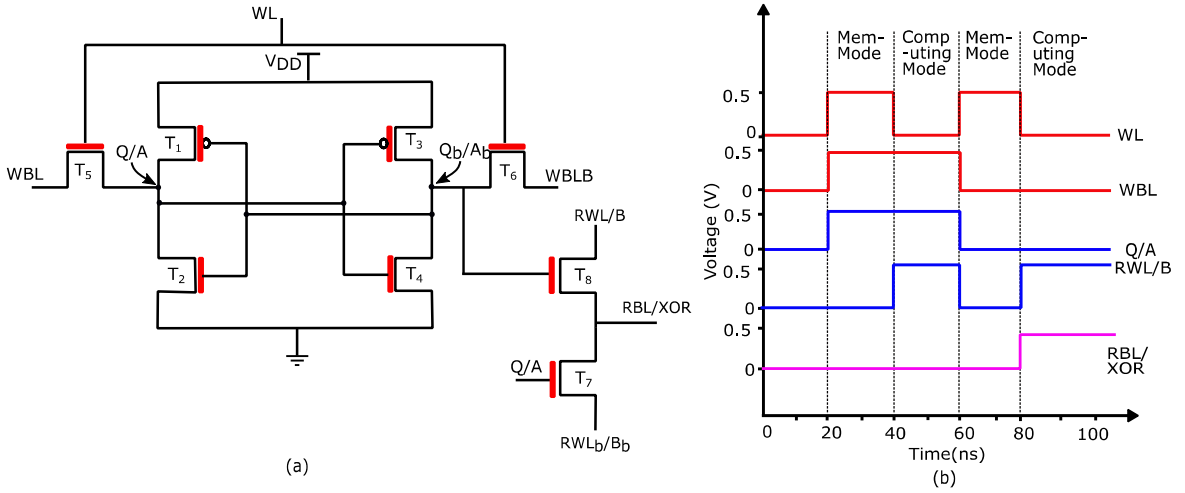

Fig. 5. (a) NCFET-based8T-SRAM CiM XOR logic design, and (b) transient response characteristics of the 8T-SRAM CiM XOR logic.

C. NCFET-based 8T-SRAM Computing-in-Memory AND Logic Design

The NCFET CiM AND logic design is shown in Figure 6(a). As illustrated in Figure 6(b), in memory mode, when the WL is high, the WBL value is stored in the memory cell, representing input A. Performing in-memory computations within the cell involves using the stored data (Q/Q_b) as input A and the RWL as input B. When carrying out the CiM AND operation, the result will be '1' when inputs A and B are '1'; otherwise, the output will be '0'. As illustrated in Figure 6(b), when WL is high, the WBL value is stored in the memory cell and is treated as input A.When WL is low, the CiM AND operation is performed between the A and the RWL input B. In computing mode,with WL low, WBL high, and RWL high, the output for the CiM AND gate is high.

Figure 7 presents a comparison of the energy consumption of the proposed NCFET 8T-SRAM CiM logic gates with non-CiM logic gates for different T_{fe} values at V_{DD}=0.5 V. Overall, the CiM designs exhibit low energy consumption, with an optimal energy consumption occurring at T_{fe}=3 nm. The 8T-SRAM-based CiM XOR, AND, and OR logic designs achieve ~2.6×, ~3× and ~3× reductions in energy consumption, respectively, compared to the non-CiM-based logic designs.

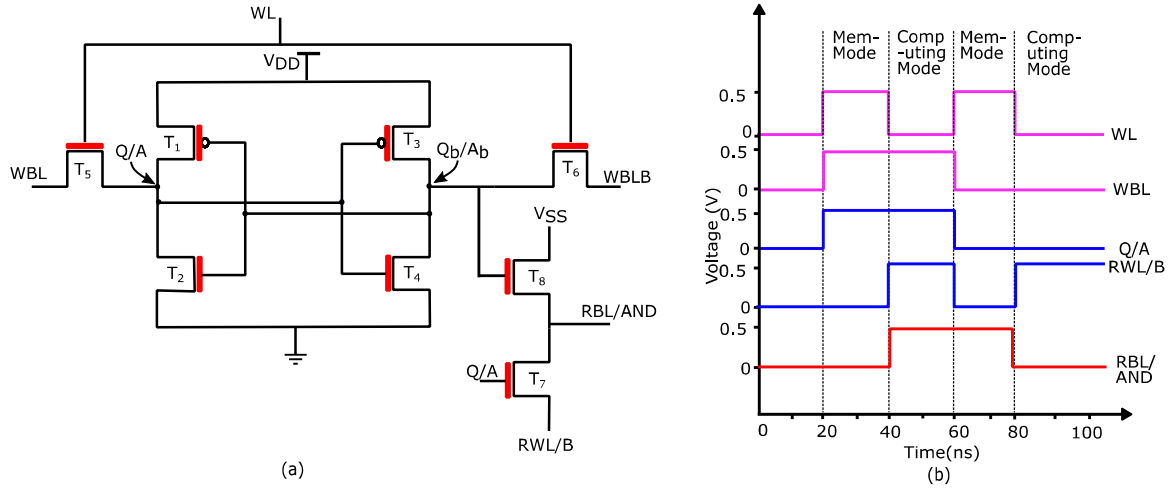

Fig. 6. (a) NCFET-based 8T-SRAM CiM AND logic design, and (b) transient response characteristics of the 8T-SRAM CiM AND logic.

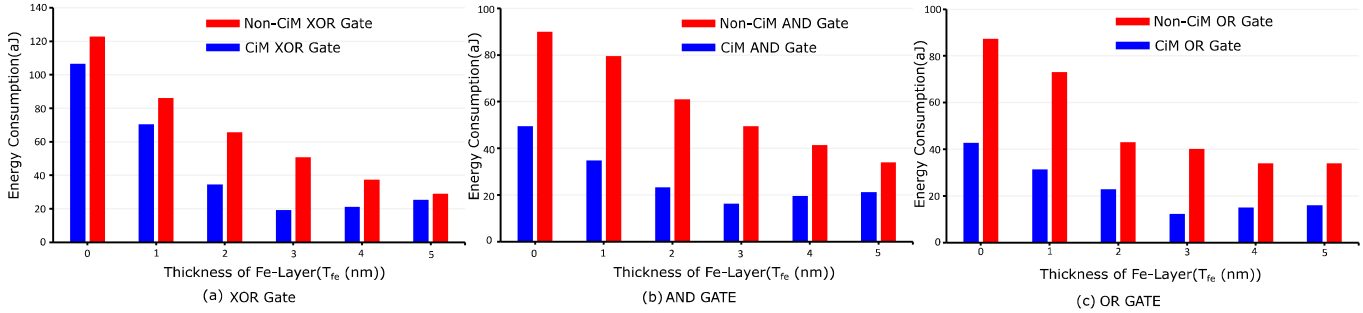

Fig. 7. Performance analysis of 8T-SRAM CiM logic gates compared to non-CiM logic gates using NCFETs with varying T_{fe} values at 0.5V:(a) XOR gate, (b) AND gate, and (c) OR gate.

IV. PROPOSED ENERGY EFFICIENT AND SECURE NCFET-BASED 8T-SRAM CIM S-BOX DESIGN FOR LIGHTWEIGHT BLOCK CIPHERS

In the context of lightweight block ciphers, the substitution box (S-box) serves as a nonlinear element, introducing confusion through its mapping input of input bits to output bits in a nonlinear fashion. An efficient S-box design is critical for enhancing the security and energy efficiency of the cipher for resource-limited IoT edge devices.

The proposed 8T-SRAM-based CiM S-box design with the reconfigurable architecture, as shown in Figure 8, enhances the energy efficiency and resiliency of lightweight block ciphers. The 8T-SRAM CiM-based SLIM S-box design has four inputs (X_3-X_0) and four outputs (Y_3-Y_0). This S-box design has been implemented using the proposed NCFET-based 8T-SRAM CiM logic gates.The following Boolean equations are used to express the relationship between inputs and outputs:

$$Y_3 = X_0 \oplus X_3.Y_0 \quad (4)$$

$$Y_2 = X_3 \oplus (X_2 + X_1) \quad (5)$$

$$Y_1 = X_1 \oplus X_0.Y_2 \quad (6)$$

$$Y_0 = X_2 \oplus X_0.X_1 \quad (7)$$

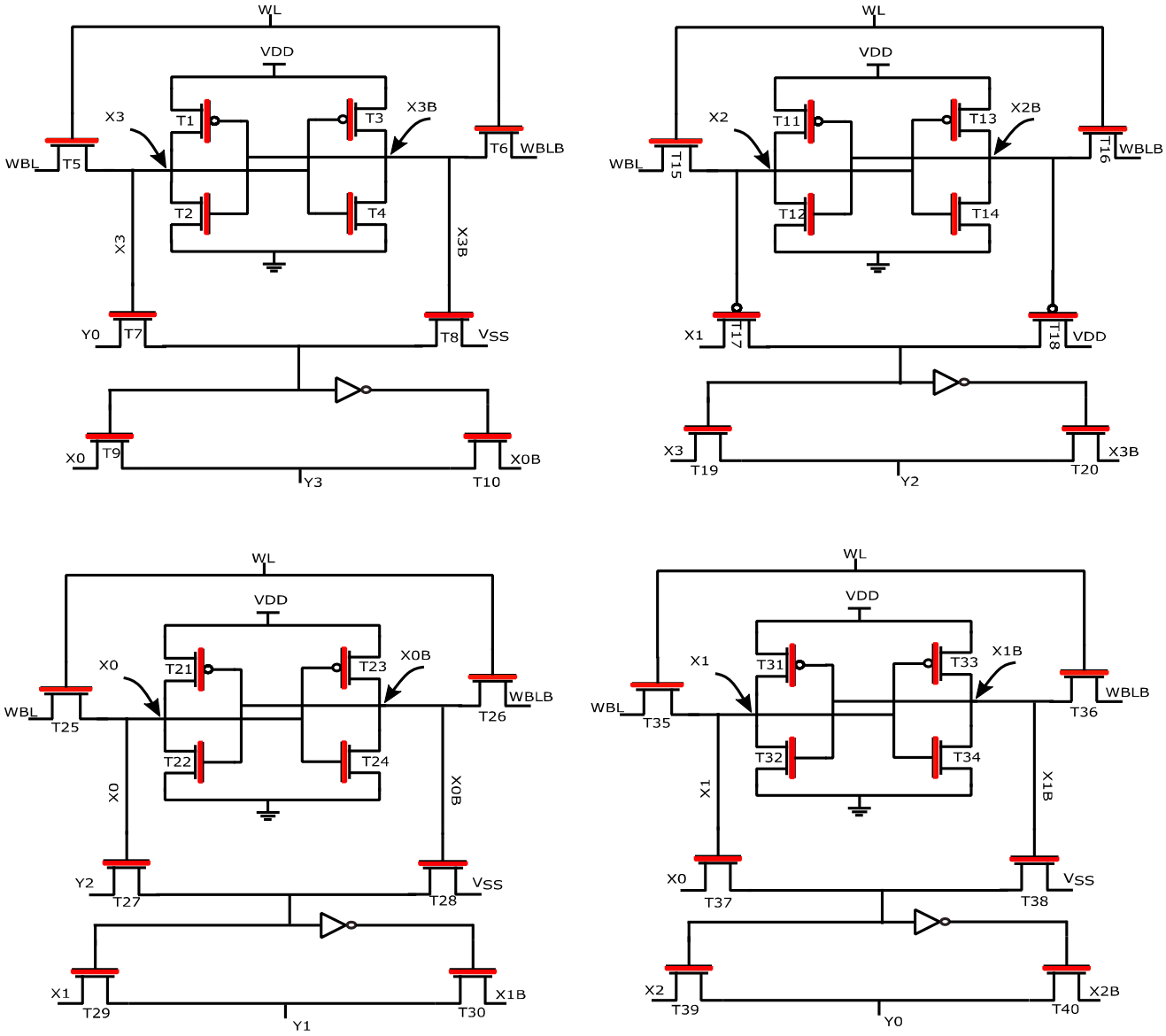

Fig. 8. Proposed NCFET-based 8T-SRAM CiM SLIM S-box design for lightweight block ciphers.

According to the above equations, when the input is $X_3X_2X_1X_0 = 0001$, the corresponding output is $Y_3Y_2Y_1Y_0 = 1000$. Figure 9 shows that the transient response characteristics of the proposed NCFET-based 8T-SRAM CiM SLIM S-box at V_{DD}=0.5 V. Here, WL represents the word line which is used to write/read data from the S-box.

As previously stated, the 8T-SRAM-based CiM S-box design is capable of operating in two distinct modes: memory mode and computing mode. When operating in memory mode, the information stored in memory cells are displayed through a write operation. To perform the write operation, the write port is activated by enabling the WL and setting the WBL/WBLB lines of the memory cells to the necessary voltage levels, as shown in Figure 10. When operating in computing mode, the S-box leverages the isolation read mechanism to perform in-memory operations within the SRAM cells, while preserving the stored data. For example, as shown in Figure 9, when the S-box is in write mode, i.e. WL is high, the input $X_3X_2X_1X_0 = 1110$ is stored in the memory cells. When in computing mode, i.e. WL is low, logic operations are performed on the stored data along with an additional external input, resulting in the output $Y_3Y_2Y_1Y_0 = 1011$.

Figure 10 presents the energy consumption comparison of the proposed NCFET-based 8T-SRAM CiM SLIM S-box design with a non-CiM-based SLIM S-box design for different T_{fe} values at V_{DD}=0.5 V. It can be observed that at an optimal T_{fe} of 3 nm, the NCFET-based 8T-SRAM CiM SLIM S box design achieves the lowestenergy consumption, which is ~4× lower than the baseline 8T-SRAM CiM-based SLIM S-box design and ~3.8× lower than the non-CiM SLIM S- box design at V_{DD}=0.5 V.

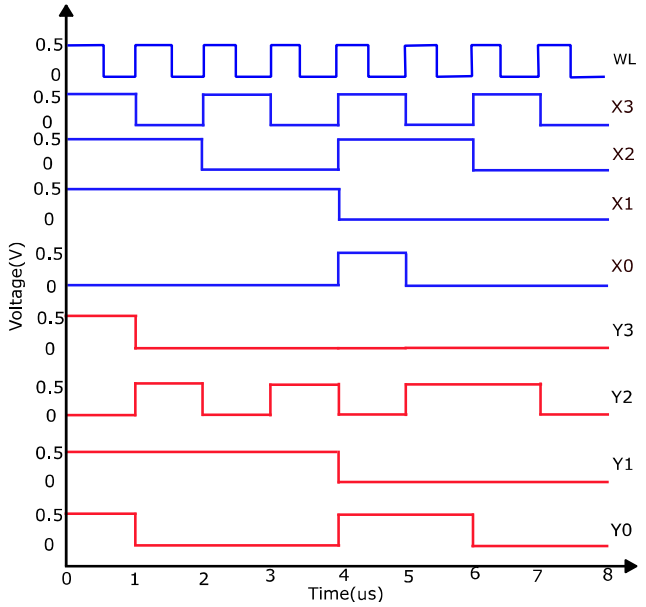

Fig. 9. Transient response characteristics of the proposed NCFET-based 8T-SRAM CiM SLIM S-box.

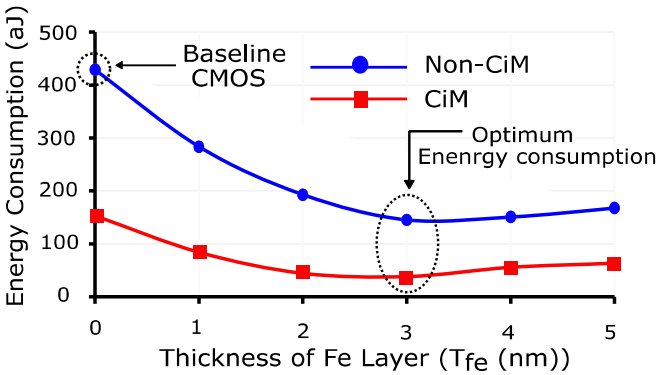

Fig. 10. Energy consumption comparison of the proposed NCFET-based 8T-SRAM CiM SLIM S-box design vs the non-CiM SLIM S-box design for varying T_{fe} values at V_{DD}=0.5V.

V. SECURITY ANALYSIS OF NCFET-BASED 8T-SRAM CIM S-BOX AGAINST DPA ATTACKS AND PERFORMANCE BENCHMARKING FOR LIGHTWEIGHT SLIM CIPHERS

A. DPA Attack Methodology on 8T-SRAM CIM S-BOX Design for Lightweight SLIM Cipher

DPA is a side-channel attack that performs correlation analysis by considering power traces from cryptographic engines to obtain hidden secret key information. In cryptographic engines, the S-box is often the target of the attacker.

The DPA attack is performed on the SLIM S-box design, as illustrated in Figure 11. The detailed DPA attack mechanism is described as follows:

- The S-box is first designed in the Cadence Virtuoso environment, and current traces (i_{Vdd}) are recorded using random inputs (X) and a fixed key (K).
- The current traces are recorded at a sampling rate of T (T samples per trace) and organized into a matrix S of dimensions X × T.
- Next, the S-box algorithm is implemented using Python 3 to calculate the output values using the same inputs X as in the previous step and all potential keys K. The output values are mapped to hypothetical power consumption values through the Hamming Distance (HD) model and organized in a matrix H with dimensions X × K. The HD between two consecutive output values is determined using (8).
- $HD = \text{Hamming Weight}(Y_{i-1} \oplus Y_i)$ (8)
- Finally, every column of matrix H is correlated with all the columns of the current trace matrix S.

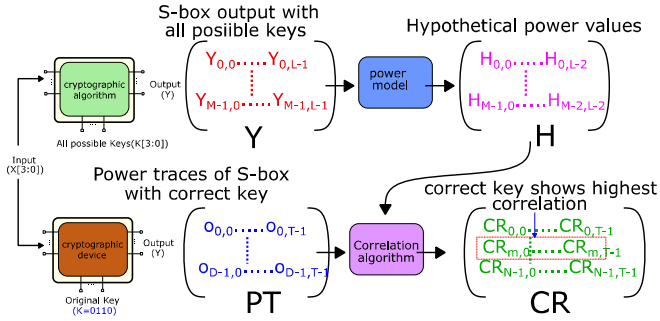

Fig. 11. DPA attack mechanism on the NCFET-based 8T-SRAM CiM SLIM S-box.

The encryption key with the highest correlation value among all keys is identified as the correct key. Figures 12(a) and 12(b) show the power/current traces recorded from the non-CiM SLIM S-box designs with baseline CMOS and NCFET technologies. Figures 12(c) and 12(d) present the current traces for the CiM-based S-box designs using baseline CMOS and NCFET at V_{DD}=0.5V. It can be observed that the power traces of the NCFET-based 8T-SRAM CiM S-box design exhibits reduced data-dependent current variations compared to both baseline CMOS and non-CiM designs. This reduction can be attributed to the reconfigurable nature of the CiM architecture, combined with the NCFET non-linear current traces, due to higher power consumption values.

Figure13 further illustrates and compares the correlation coefficient of the NCFET-based 8T-SRAM CiM SLIM S-box design with a T_{fe} of 3 nm with the baseline CiM S-box design, considering 32 power traces.The original key (K = 0110) is represented as a dotted line to distinguish it from any incorrect key guesses. The correlation coefficients for the baseline CiM S-box design with all possible keys can be observed in Figure 13(a). The DPA attack successfully targets the baseline CiM S-box design, achieving the highest correlation with the original key after evaluating just 32 power traces. This demonstrates that the baseline CiM S-box design is more vulnerable to DPA attacks, as the original key can be retrieved with only 32 power

traces. In contrast, the DPA attack performed on the NCFET-based 8T-SRAM CiM SLIM S-box was unsuccessful across a range of T_{fe} values (1 nm to 5 nm). Figure 13(b) shows that, at T_{fe}=3 nm, the DPA attack on the NCFET-based 8T-SRAM CiM SLIM S-box fails with 32 power traces, demonstrating its higher resiliency. Furthermore, a DPA attack is conducted on the NCFET-based 8T-SRAM CiM S-box, with a varying number of power traces (64, 128, 192, 256, 512). Figure 14 illustrates the correlation coefficient of the NCFET-based 8T-SRAM CiM S-box for 1024 power traces and a varying T_{fe}, ranging from 1 nm to 5 nm. According to the analysis, DPA attack has proven to be successful in targeting the NCFET-based 8T-SRAM CiM S-box design with 1024 power traces, for T_{fe} values of 1 nm, 2 nm, 4 nm, and 5 nm. Furthermore, the DPA attack when T_{fe}=3 nm proved unsuccessful with 1024 power traces. This highlights the enhanced resilience of the NCFET-based 8T-SRAM CiM S-box against DPA, as depicted in Figures 14(c). Consequently, the DPA attack successfully targets the NCFET-based 8T-SRAM CiM S-box with 1024 power traces, whereas the DPA attack on baseline 8T-SRAM CiM S-box is compromised with just 32 power traces. Consequently, the attack effort ratio for DPA has been increased by 32 times, thereby enhancing the resistance of the NCFET-based 8T-SRAM CiM S-box design.

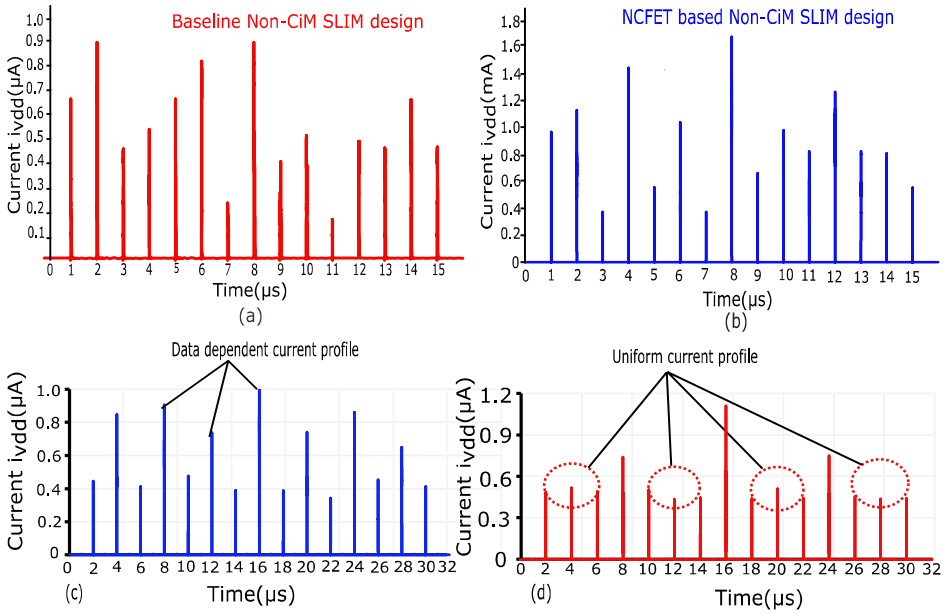

Fig. 12. Current traces demonstrating data dependency: (a) baseline CMOS non-CiM SLIM S-box design, (b) NCFET-based non-CiM SLIM S-box design, (c) baseline CMOS CiM S-box design, and (d) NCFET-based CiM S-box design.

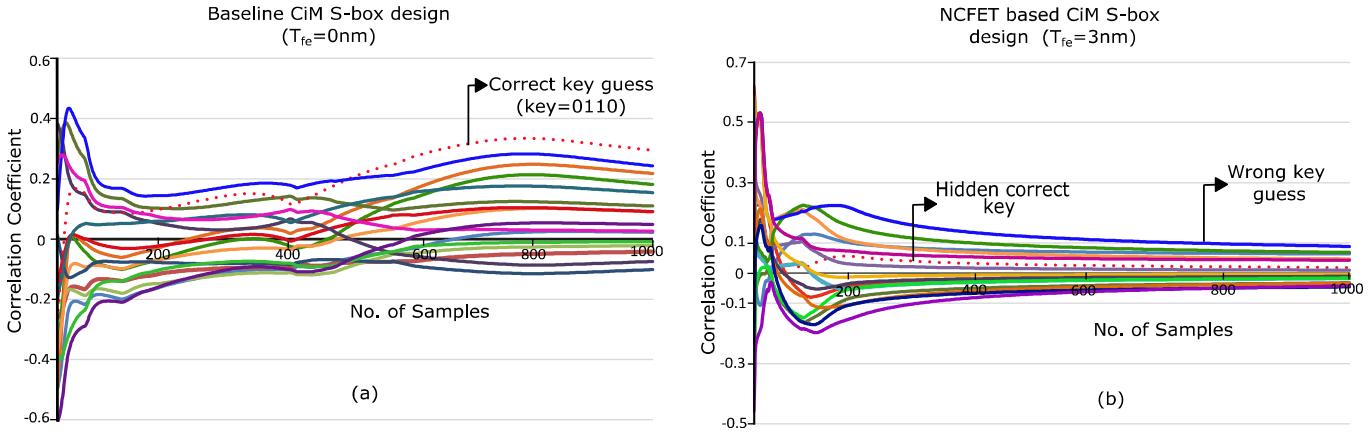

Fig. 13. Correlation coefficient analysis of 8T-SRAM CiM SLIM S-box design with: (a) baseline CiM S-box design (T_{fe}=0 nm), and (b) NCFET-based CiM S-box design at T_{fe}=3 nm, using 32 power traces at V_{DD}=0.5 V.

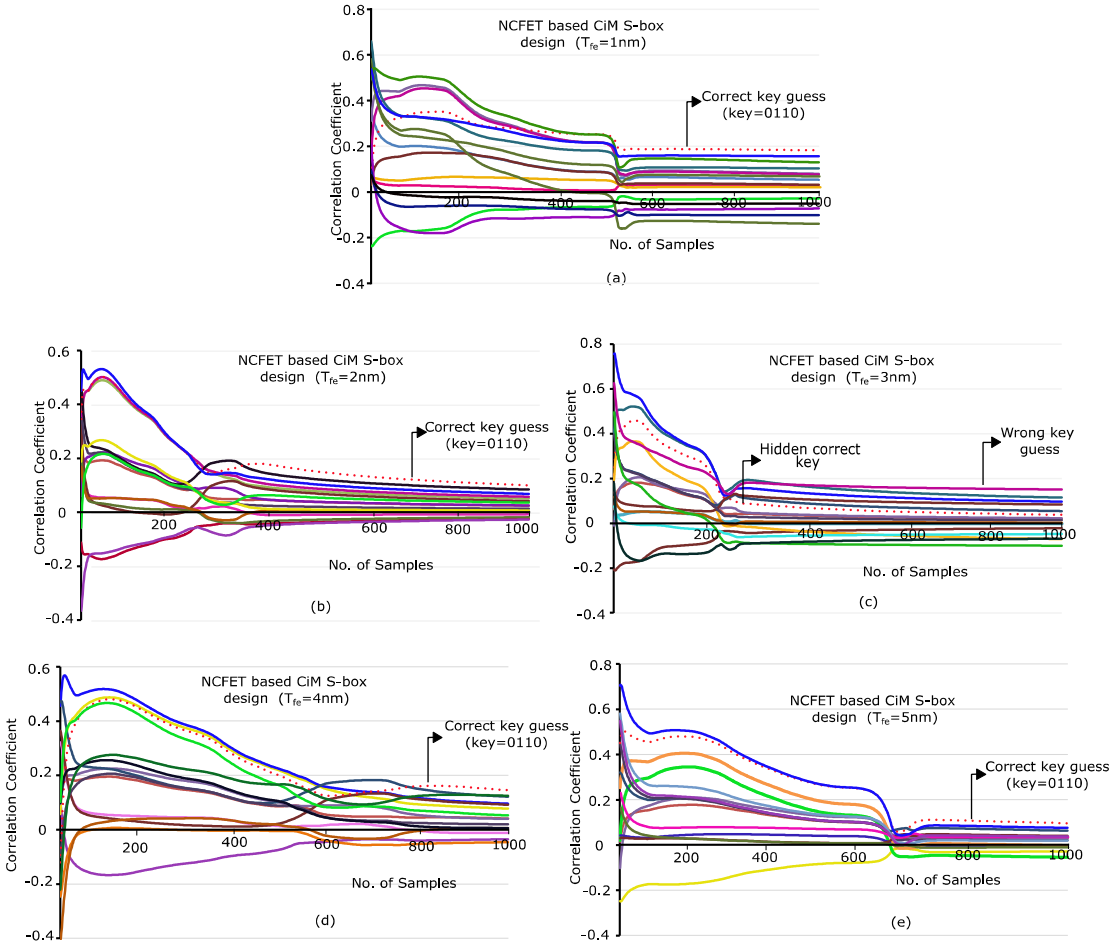

Fig. 14. Correlation coefficient analysis of the NCFET-based 8T-SRAM CiM SLIM S-box design using 1024 power traces atV_{DD}=0.5V, for: (a)T_{fe}=1nm, (b)T_{fe}=2nm, (c)T_{fe}=3nm, d)T_{fe}=4nm, and (e)T_{fe}=5nm.

B. Performance Benchmarking of the Proposed NCFET-based 8T-SRAM CiM SLIM S-BOX Design

This section presents the overall performance benchmarking of the proposed NCFET-based 8T-SRAM CiM S-box design, considering important performance metrics for DPA attacks. The parameters considered and analyzed are as follows.

1) Signal-to-Noise Ratio

Signal-to-Noise Ratio (SNR) can be described as the ratio between the correlation value of the correct key and the second highest value of an incorrect key guess, as shown in (9) [33].

$$\text{SNR} = \frac{\text{Correlation of the correct key}}{\text{Second highest value of wrong key guess}} \quad (9)$$

To demonstrate resiliency against DPA attacks, it is essential to estimate the SNR value. A high level of robustness against DPA attacks is indicated by a lower SNR value in the S-box. Additionally, SNR plays a crucial role in determining the degree of difficulty in distinguishing between the correct key and an incorrect key guess.

Figure 15 illustrates the variation in the SNR value of the 8T-SRAM CiM SLIM S-box design as a function of the FE layer thickness (T_{fe}). As T_{fe}increases, a reduction in the SNR value is observed. The reconfigurable nature and suppressed power consumption values of the proposed NCFET-based 8T-SRAM CiM SLIM S-box design result in lower SNR values and higher resiliency for DPA attacks. The proposed design achieves an SNR value ~2.2× lower than the baseline CiM SLIM S-box design and 1.5× lower than the NCFET-based non-CiM S-box design under similar design constraints.

2) Measurements to Disclosure

According to [34], the Measurements to Disclosure (MTD) is defined as the intersection of the correlation coefficient of the correct key with the highest correlation coefficient of all incorrect key guesses. The MTD value represents the robustness of an S-box against DPA attacks. A higher MTD value indicates greater robustness. Figure 16 presents the MTD values for the 8T-SRAM CiM SLIM S-box design using both baseline CMOS and NCFET technologies. It can be observed that the MTD value of the NCFET-based 8T-SRAM CiM SLIM S-box design is higher than that of the baseline CMOS design. The MTD value of the proposed NCFET-based 8T-

SRAM CiM SLIM S-box design is ~32 times higher than that of the baseline CMOS-based design, and ~4 times higher than that of the NCFET-based non-CiM S-box design, under similar design constraints.

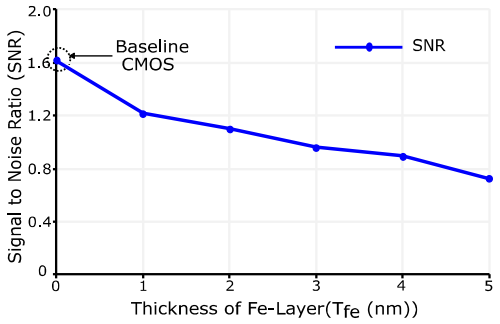

Fig. 15. SNR analysis of the NCFET-based 8T-SRAM CiM SLIM S-box with varyingT_{fe} values.

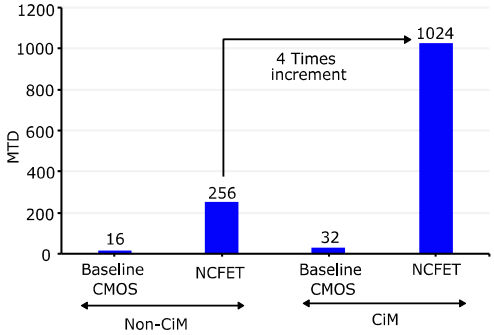

Fig. 16. MTD analysis of non-CiM and CiM-based SLIM S-box designs using baseline CMOS and NCFET technologies.

3) Security Power Delay

The Security Power Delay (SPD) metric is employed to evaluate the trade-off between security and system efficiency [35]. This figure of merit, calculated using (10), assesses the trade-off between security, power consumption, and timing performance.

$$SPD = \frac{MTD}{(Power * Delay)} \quad (10)$$

It is important to note that the SDP metric is only applicable when the system has been evaluated as secure enough to be utilized in cryptographic hardware applications. As shown in Figure 17, the SDP value of the proposed NCFET-based 8T-SRAM CiM SLIM S-box design is ~43.4× higher than that of the equivalent baseline CMOS CiM design, and ~8.1× higher than that of the NCFET-based non-CiM S-box design under similar design constraints.

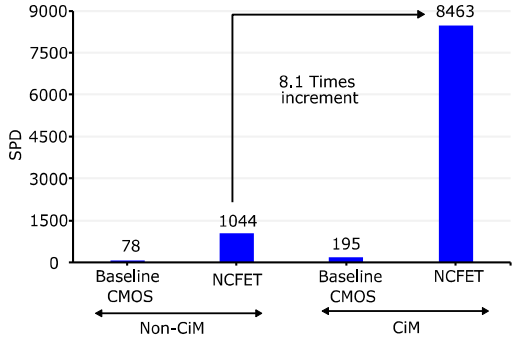

Fig. 17. SPD analysis of non-CiM & CiM-based SLIM S-box designs using baseline CMOS and NCFET technologies.

Table IV summarizes and benchmark the performance of the proposed NCFET-based 8T-SRAM CiM SLIM S-box design against the baseline CMOS CiM design and other state-of-the-art non-CiM S-box designs. Overall, it can be observed that the proposed design is highly energy efficient and robust to DPA attacks when compared to these designs. The proposed NCFET-based 8T-SRAM CiM S-box design has ~3.8× lower energy consumption when compared to the NCFET-based non-CiM S-box design and ~4× lower energy consumption when compared to the baseline CMOS CiM S- box design.

TABLE IV. PERFORMANCE BENCHMARKING OF THE PROPOSED NCFET-BASED 8T-SRAM CIM SLIM S-BOX DESIGN AGAINST BASELINE CMOS CIM AND OTHER STATE-OF-THE-ART NON-CIM S-BOX DESIGNS

	Non-CiM PRIDE S-box[35]	**Non-CiMPRIDES-box[35]**	**Non-CiM Sbox9[36]**	**Non- CiM PRESENT-80 S-box[21]**	**Non-CiM S-box[37]**	**Non-CiMS-box[37]**	**CiM S-box [This work]**	**CiM S-box [This work]**
Technology	FinFET-14nm	HyperFET-14nm	TSMC-90nm CMOS	NCFET-40nm	CMOS-40nm	NCFET-40nm	CMOS-40nm	NCFET-40nm
V_{DD}(V)	0.8	0.8	1.2	0.5	0.5	0.5	0.5	0.5
Power consumption(uW)	5.04	5.16	—	0.254	0.085	0.544	0.075	0.336
Propagation delay (ns)	0.18	0.52	—	0.51	3.54	0.45	2.26	0.36
Energy consumption(fJ)	1.81	5.36	—	0.259	0.608	0.490	0.390	0.242
PDP (fJ)	0.895	2.689	678.27	0.129	0.205	0.245	0.195	0.121
Attack effort ratio	—	12	—	64	16	256	32	1024
SNR	—	—	—	0.795	1.107	0.298	0.897	0.198
MTD	76.06	—	303	64	16	256	32	1024
SPD (10^{15}) J^{-1}	85.83	711.36	0.44	275	78	1044	195	8463

The attacker effect ratio of the proposed NCFET-based 8T-SRAM CiM SLIM S-box design is 4× higher than that of the non-CiM SLIM S-box with NCFET and 32× higher than the baseline CiM S-box design. The SNR value achieved by the proposed design is ~2.2× lower than that of the baseline CiM SLIM S-box design and 1.5× lower than that of the the NCFET-based non-CiM S-box design, under similar design constraints. The MTD value of the proposed design is ~32 times higher than that of the 8T-SRAM CiM SLIM S-box design using baseline CMOS and ~4 times higher than that of the NCFET-based non-CiM S-box design, under similar design constraints. Furthermore, the SPD value of the proposed design is ~43.4× higher than that of the equivalent baseline CMOS CiM design and ~8.1× higher than that of the NCFET-based non-CiM S-box design, under similar design constraints. These results demonstrate the superior capability of NCFET-based CiM architectures in enhancing hardware security and trustworthiness of lightweight ciphers used in edge AI devices.

VI. CONCLUSION

This work proposes and demonstrates an energy efficient and robust Negative Capacitance Field-Effect Transistor (NCFET)-based 8T-SRAM Computing-in-Memory (CiM) cell and CiM logic gates for lightweight cipher applications. We further demonstrate an 8T-SRAM CiM lightweight SLIM cipher S-box that exploits NCFETs to achieve enhanced energy efficiency. In addition, we present a hardware security evaluation of the proposed 8T-SRAM CiM-based S-box design for Differential Power Analysis (DPA) attacks. Performance benchmarking is also conducted against state-of-the-art CiM and non-CiM designs.

It has been demonstrated that the reconfigurable nature of the proposed CiM architecture, combined with the unique steep slope characteristics of NCFETs, enhances the overall S-box design's DPA resiliency and energy efficiency. The proposed NCFET-based 8T-SRAM CiM S-box design exhibits ~3.8× lower energy consumption in comparison to the non-CiM NCFET S-box design and ~4× lower energy consumption in comparison to the baseline CMOS CiM S-box design. The reconfigurable nature and reduced power consumption of the proposed NCFET 8T-SRAM CiM SLIM S-box design result in lower Signal-to-Noise Ratio (SNR) values and higher resiliency for DPA attacks. The security evaluation of the proposed design for DPA attacks demonstrates a 32× increase in the attacker effect ratio, a ~2.2× reduction in SNR, a ~43.4× improvement in the Security Power Delay (SPD), and a 32× increase in the Measurements to Disclosure (MTD). Furthermore, the SPD value of the proposed design is ~43.4× higher than that of the equivalent baseline CMOS CiM design and ~8.1×higher than that of the NCFET-based non-CiM S-box design under similar design constraints. These results clearly demonstrate the higher suitability of NCFET-based CiM structures for enhancing hardware security and the trustworthiness of lightweight ciphers used in edge Artificial Intelligence (AI) devices.

REFERENCES

[1] T. A. Win, "Enhancing Security in On-Chip Communication: A Survey of Threats and Solutions,"*Journal of IoT in Social, Mobile, Analytics, and Cloud*, vol. 6, no. 3, pp. 240–253, Jul. 2024.

[2] F. Li, A. Shinde, Y. Shi, J. Ye, X.-Y. Li, and W. Song, "System Statistics Learning-Based IoT Security: Feasibility and Suitability,"*IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6396–6403, Aug. 2019, https://doi.org/10.1109/JIOT.2019.2897063.

[3] M. Bartock *et al.*, "Hardware-Enabled Security for Server Platforms: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases (Withdrawn)," U.S. Department of Commerce, NIST CSWP 14, Apr. 2020. https://doi.org/10.6028/NIST.CSWP.14.ipd.

[4] S. Roshanisefat, H. M. Kamali, H. Homayoun, and A. Sasan, "SAT-Hard Cyclic Logic Obfuscation for Protecting the IP in the Manufacturing Supply Chain,"*IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 28, no. 4, pp. 954–967, Apr. 2020, https://doi.org/10.1109/TVLSI.2020.2968552.

[5] P. Prinetto and G. Roascio, "Hardware Security, Vulnerabilities, and Attacks: A Comprehensive Taxonomy," in *Proceedings of the Fourth Italian Conference on Cyber Security*, Ancona, Italy, 2020.

[6] P. De, C. Mandal, and U. Prampalli, "Path-Balanced Logic Design to Realize Block Ciphers Resistant to Power and Timing Attacks,"*IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 5, pp. 1080–1092, May 2019, https://doi.org/10.1109/TVLSI.2019.2896377.

[7] H. Mestiri, "Evaluating AES Security: Correlation Power Analysis Attack Implementation using the Switching Distance Power Model,"*Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 20314–20320, Feb. 2025, https://doi.org/10.48084/etasr.9728.

[8] H. Mestiri, I. Barraj, and M. Machhout, "Innovative Fault Detection for AES in Embedded Systems: Advancing Resilient and Sustainable Digital Security,"*Engineering, Technology & Applied Science Research*, vol. 15, no. 2, pp. 20660–20667, Apr. 2025, https://doi.org/10.48084/etasr.9852.

[9] W. Wang, Y. Yu, F.-X. Standaert, J. Liu, Z. Guo, and D. Gu, "Ridge-Based DPA: Improvement of Differential Power Analysis For Nanoscale Chips,"*IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1301–1316, May 2018, https://doi.org/10.1109/TIFS.2017.2787985.

[10] D. Rossi, V. Tenentes, S. Yang, S. Khursheed, and B. M. Al-Hashimi, "Aging Benefits in Nanometer CMOS Designs,"*IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 64, no. 3, pp. 324–328, Mar. 2017, https://doi.org/10.1109/TCSII.2016.2561206.

[11] T. De Cnudde and S. Nikova, "Securing the PRESENT Block Cipher Against Combined Side-Channel Analysis and Fault Attacks,"*IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 12, pp. 3291–3301, Dec. 2017, https://doi.org/10.1109/TVLSI.2017.2713483.

[12] M. Masoumi, "Novel Hybrid CMOS/Memristor Implementation of the AES Algorithm Robust Against Differential Power Analysis Attack,"*IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 7, pp. 1314–1318, Jul. 2020, https://doi.org/10.1109/TCSII.2019.2932337.

[13] N. Arya, T. Soni, M. Pattanaik, and G. K. Sharma, "Area and Energy Efficient Approximate Square Rooters for Error Resilient Applications," in *2020 33rd International Conference on VLSI Design and 2020 19th International Conference on Embedded Systems*, Bangalore, India, 2020, pp. 90–95, https://doi.org/10.1109/VLSID49098.2020.00033.

[14] Y. Liu, K. Qian, K. Wang, and L. He, "Effective Scaling of Blockchain Beyond Consensus Innovations and Moore's Law: Challenges and Opportunities,"*IEEE Systems Journal*, vol. 16, no. 1, pp. 1424–1435, Mar. 2022, https://doi.org/10.1109/JSYST.2021.3087798.

[15] Y.-C. Chien, H. Xiang, J. Wang, Y. Shi, X. Fong, and K.-W. Ang, "Attack Resilient True Random Number Generators Using Ferroelectric-Enhanced Stochasticity in 2D Transistor,"*Small*, vol. 19, no. 38, Sep. 2023, Art. no.2302842, https://doi.org/10.1002/smll.202302842.

[16] S. D. Kumar and H. Thapliyal, "Exploration of Non-Volatile MTJ/CMOS Circuits for DPA-Resistant Embedded Hardware,"*IEEE Transactions on Magnetics*, vol. 55, no. 12, pp. 1–8, Dec. 2019, https://doi.org/10.1109/TMAG.2019.2943053.

[17] H. Amrouch, V. M. van Santen, G. Pahwa, Y. Chauhan, and J. Henkel, "NCFET to Rescue Technology Scaling: Opportunities and Challenges," in *2020 25th Asia and South Pacific Design Automation Conference*,

Beijing, China, 2020, pp. 637–644, https://doi.org/10.1109/ASP-DAC47756.2020.9045415.

[18] R. C. Bheemana, A. Japa, S. Yellampalli, and R. Vaddi, "Steep Switching NCFET based Logic for Future Energy Efficient Electronics," in *2021 IEEE International Symposium on Smart Electronic Systems*, Jaipur, India, 2021, pp. 327–330, https://doi.org/10.1109/iSES52644.2021.00083.

[19] C.-H. Lee, Y.-T. Hsu, T.-T. Liu, and T.-D. Chiueh, "Design of an 45nm NCFET Based Compute-in-SRAM for Energy-Efficient Machine Learning Applications," in *2020 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, Ha Long, Vietnam, 2020, pp. 193–196, https://doi.org/10.1109/APCCAS50809.2020.9301709.

[20] C.-C. Fan, C.-H. Cheng, Y.-R. Chen, C. Liu, and C.-Y. Chang, "Energy-efficient HfAlOx NCFET: Using gate strain and defect passivation to realize nearly hysteresis-free sub-25mV/dec switch with ultralow leakage," in *2017 IEEE International Electron Devices Meeting*, San Francisco, CA, USA, 2017, p. 23.2.1-23.2.4, https://doi.org/10.1109/IEDM.2017.8268444.

[21] R. C. Bheemana, A. Japa, S. sankar Yellampalli, and R. Vaddi, "Negative capacitance FET based energy efficient and DPA attack resilient ultra-light weight block cipher design,"*Microelectronics Journal*, vol. 133, Mar. 2023, Art. no.105711, https://doi.org/10.1016/j.mejo.2023.105711.

[22] S. Huang, H. Jiang, X. Peng, W. Li, and S. Yu, "XOR-CIM: compute-in-memory SRAM architecture with embedded XOR encryption," in *Proceedings of the 39th International Conference on Computer-Aided Design*, New York, NY, USA, 2020, pp. 1–6, https://doi.org/10.1145/3400302.3415678.

[23] K. S and B. S. Reniwal, "In-Memory Encryption using XOR-based Feistel Cipher in SRAM Array," in *2024 IEEE International Symposium on Circuits and Systems*, Singapore, Singapore, 2024, pp. 1–5, https://doi.org/10.1109/ISCAS58744.2024.10558309.

[24] C.-Y. Hsieh, S.-T. Lin, Z. Li, C.-C. Lu, M.-F. Chang, and K.-T. Tang, "MARSv2: Multicore and Programmable Reconstruction Architecture SRAM CIM-Based Accelerator with Lightweight Network," in *2022 IEEE 4th International Conference on Artificial Intelligence Circuits and Systems*, Incheon, Republic of Korea, 2022, pp. 383–386, https://doi.org/10.1109/AICAS54282.2022.9870005.

[25] Z. Lin *et al.*, "In Situ Storing 8T SRAM-CIM Macro for Full-Array Boolean Logic and Copy Operations,"*IEEE Journal of Solid-State Circuits*, vol. 58, no. 5, pp. 1472–1486, May 2023, https://doi.org/10.1109/JSSC.2022.3206318.

[26] Z. Lin *et al.*, "A review on SRAM-based computing in-memory: Circuits, functions, and applications,"*Journal of Semiconductors*, vol. 43, no. 3, Mar. 2022, Art. no.031401, https://doi.org/10.1088/1674-4926/43/3/031401.

[27] X. Li *et al.*, "A 9T-SRAM based computing-in-memory with redundant unit and digital operation for boolean logic and MAC,"*Microelectronics Journal*, vol. 145, Mar. 2024, Art. no.106124, https://doi.org/10.1016/j.mejo.2024.106124.

[28] Z. Wang, H. Luo, Z. Peng, X. Chao, and Y. He, "An 8T SRAM Based Digital Compute-In-Memory Macro For Multiply-And-Accumulate Accelerating," in *2023 IEEE International Symposium on Circuits and Systems*, Monterey, CA, USA, 2023, pp. 1–5, https://doi.org/10.1109/ISCAS46773.2023.10182037.

[29] P.-C. Wu *et al.*, "A 28nm 1Mb Time-Domain Computing-in-Memory 6T-SRAM Macro with a 6.6ns Latency, 1241GOPS and 37.01TOPS/W for 8b-MAC Operations for Edge-AI Devices," in *2022 IEEE International Solid-State Circuits Conference*, San Francisco, CA, USA, 2022, pp. 1–3, https://doi.org/10.1109/ISSCC42614.2022.9731681.

[30] V. Birudu, S. S. Yellampalli, and R. Vaddi, "A negative capacitance FET based energy efficient 6T SRAM computing-in-memory (CiM) cell design for deep neural networks,"*Microelectronics Journal*, vol. 139, Sep. 2023, Art. no.105867, https://doi.org/10.1016/j.mejo.2023.105867.

[31] U. Radhakrishna, A. Khan, S. Salahuddin, and D. Antoniadis, "Compact model of negative capacitance MOSFETs (NCFETs)," MIT, Georgia Tech, Univ. California, Berkeley, Berkeley, CA, USA, Tech. Rep, Technical report, 2017.

[32] G. Pahwa *et al.*, "Analysis and Compact Modeling of Negative Capacitance Transistor with High ON-Current and Negative Output Differential Resistance—Part II: Model Validation,"*IEEE Transactions on Electron Devices*, vol. 63, no. 12, pp. 4986–4992, Dec. 2016, https://doi.org/10.1109/TED.2016.2614436.

[33] S. D. Kumar, H. Thapliyal, and A. Mohammad, "FinSAL: FinFET-Based Secure Adiabatic Logic for Energy-Efficient and DPA Resistant IoT Devices,"*IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 1, pp. 110–122, Jan. 2018, https://doi.org/10.1109/TCAD.2017.2685588.

[34] K. Tiri *et al.*, "Prototype IC with WDDL and Differential Routing – DPA Resistance Assessment," in *Cryptographic Hardware and Embedded Systems – CHES 2005: 7th International Workshop*, Edinburgh, UK, 2005, pp. 354–365, https://doi.org/10.1007/11545262_26.

[35] I. M. Delgado-Lozano, E. Tena-SÁnchez, J. NÚÑez, and A. J. Acosta, "Design and Analysis of Secure Emerging Crypto-Hardware Using HyperFET Devices,"*IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 2, pp. 787–796, Apr. 2021, https://doi.org/10.1109/TETC.2020.2977735.

[36] E. Tena-Sánchez and A. J. Acosta, "Logic minimization and wide fan-in issues in DPL-based cryptocircuits against power analysis attacks,"*International Journal of Circuit Theory and Applications*, vol. 47, no. 2, pp. 238–253, 2019, https://doi.org/10.1002/cta.2587.

[37] K. R. Penumalli, V. Gonuguntla, and R. Vaddi, "An Energy Efficient and DPA Attack Resilient NCFET-Based S-Box Design for Secure and Lightweight SLIM Ciphers,"*Electronics*, vol. 14, no. 6, Mar. 2025, Art. no. 1114, https://doi.org/10.3390/electronics14061114.